Quantum correlations, certifying quantum devices, and the quest for infinite entanglement

Thesis by
Andrea Wei Coladangelo

In Partial Fulfillment of the Requirements for the
Degree of
Doctor of Philosophy in Computing and Mathematical Sciences

CALIFORNIA INSTITUTE OF TECHNOLOGY
Pasadena, California

2020
Defended 18 November 2019

Andrea Wei Coladangelo
ORCID: 0000-0002-6773-2711

ACKNOWLEDGEMENTS

I have had a very happy and fulfilling time during my PhD. For this, I owe thanks to many people.

First of all, I thank my advisor Thomas Vidick: for being an example to me, both scientifically and professionally; for always being available to meet whenever I asked (often on the same day); for being ridiculously prompt in replying to my emails with all forms of advice, feedback, guidance; at the same time, for mostly letting me be on my own whenever I did not reach out; for giving me unconditional freedom to explore my own research directions, while always being interested in hearing my thoughts and putting them to scrutiny; for encouraging me to travel in the summer of my first year; for providing extremely detailed feedback on the *many* drafts I sent him over the years (my writing is so much better because of this - any outstanding mediocre writing in this thesis is entirely due to me); for being a better advisor than I could imagine.

I thank the other members of my PhD committee, Fernando Brandao, Xie Chen and John Preskill, for taking the time to share their perspectives about life and the future.

I thank Valerio Scarani, for hosting my first research visit in Singapore, and for giving me a research problem that has greatly influenced this PhD thesis. Looking back, I think this is where it all started. I also thank Toni Acín, David Gosset, John Smolin, Chinmay Nirkhe, Rotem Arnon-Friedman, Umesh Vazirani, William Slofstra, Carl Miller, Mark Zhandry, Vinod Vaikuntanathan, for hosting me on fruitful visits.

I have been fortunate to have many collaborators over the years, from whom I have learned a lot: Koon Tong Goh, Valerio Scarani, Ivan Šupić, Remik Augusiak, Toni Acín, Alex Grilo, Stacey Jeffery, Thomas Vidick, Jalex Stark, Tina Zhang, Debbie Leung. Thank you for showing me that research is more fun when it is collaborative.

Going back a bit further, I feel fortunate to have had great mentors at all times. At Oxford: I am grateful to Andrew Hodges for encouraging me to do research, and to Nick Woodhouse for inviting me (and my tutorial partner Will) to his house to teach us special relativity. In high school: I thank Prof. Cimento, for being an exceptional math teacher.

I thank the members of Thomas Vidick's group over the years, for being so nice to be around, and for the many dinners at Namaste: Alex, Anand, Andru, Ben Lee, Chinmay, Jalex, Jenish, John, Rohit, Spencer, Tina. I thank Florian for being my go-to person for mathematical emergencies. From the summer we spent at the IBM quantum computing group, I thank Chris, Kanav, Leo, Pranav, Tongyang, for widening my perspective on quantum computing through many lunches and coffee breaks. I thank the friends of the "ICFO chalet", for making me feel so welcome during my visit to Barcelona.

Thanks to my best friends from the group "Grazie Ema", who have been a constant in my life since high school, despite the physical distance: Cremi, Crespi, Ema, Monti, Mula. I thank my friend Matteo, whom I have known since primary school, and whose friendship I cherish. I also thank Jenish Mehta (who cannot fathom that I will be a *Doctor of Philosophy*), for being a special friend since the start of this PhD.

The biggest thanks goes to my parents. To my dad, for being so great of a teacher that I have surpassed him in all the things he has taught me. To my mom, for being the most selfless person I know. To both, for their unwavering support in everything I do, without which this endevour would not have been possible.

Finally, to Jing Yu, bao bao, thank you for making this journey infinitely more meaningful, and for being the person I want to spend the time of the universe with.

ABSTRACT

Quantum information has the potential to disrupt the present computational landscape. Much of this potential rests on the existence of efficient quantum algorithms for classically intractable problems and of quantum cryptographic protocols for tasks that are provably impossible to realize classically. At the heart of many quantum advantages is one of the most counterintuitive features of quantum mechanics, known as *entanglement*. The central motivating question of this thesis is the following: if quantum devices will perform tasks that are beyond the reach of classical devices, can we hope to certify that they are performing these tasks correctly? Bell's theorem, a landmark result in physics, provides a partial answer to this question: it asserts that measurements on spatially isolated, but *entangled*, particles can result in outcomes that are correlated in a way that cannot be explained by any local hidden variable theory (such as Newtonian physics). A direct operational consequence of this theorem is that one can devise a statistical test to certify the presence of entanglement (and hence of genuine quantumness). Remarkably, nature allows us to take this certification one step further: in some cases, the correlation of measurement outcomes is sufficient to single out a *unique* quantum setup compatible with this correlation. This phenomenon is often referred to as self-testing, and is the central topic of this thesis. In recent years, the theory of self-testing has developed significantly, and has found many applications in quantum cryptography, in the complexity of multiprover interactive proofs, as well as strong connections to foundational questions in the theory of entanglement.

In the first part of this thesis, we review the basic terminology and results in the theory of self-testing. We then explore a concrete application to the problem of verifiably delegating a quantum computation. Our main technical contribution is a test that robustly certifies products of single-qubit Clifford measurements on many EPR pairs. We employ this test to obtain a protocol which allows a classical user to verifiably delegate her quantum computation to two spatially isolated quantum servers. The overall complexity of our protocol is near-optimal, requiring resources that scale as $O(g \log g)$ to delegate a quantum circuit of g gates.

In the second part of this thesis, the driving question is the following: what is the class of quantum states and measurements that can be certified through self-testing? Does self-testing only apply to a few special cases, like EPR pairs or copies of EPR pairs, or are these instances of a more general phenomenon? One of the main results of this thesis is that we settle this question for the case of bipartite states. We show the existence of a self-testing correlation for *any* pure bipartite entangled state of any finite local dimension. We then move on to explore the multipartite case, and we show that a significantly larger class of states can be self-tested than was previously known. This includes all multipartite partially entangled GHZ states, and all multipartite qudit states which

admit a Schmidt decomposition.

In the final part of this thesis, we explore connections of the theory of self-testing to basic questions about entanglement and quantum correlation sets. In particular, we set out to understand the expressive power of infinite-dimensional quantum systems. We consider two questions: can spatially isolated quantum systems of infinite dimension produce correlations that are unattainable by finite-dimensional systems? Does there exist a correlation that cannot be attained exactly by spatially isolated quantum systems (not even infinite-dimensional ones), but can be approximated arbitrarily well by a sequence of finite or infinite-dimensional systems? The first question was posed by Tsirelson in 1993, and its answer has been elusive. One of the main results of this thesis is a resolution of this question. We provide an explicit example of a correlation that is attained (exactly) only by infinite-dimensional systems. The second question is better known as the "non-closure of the set of quantum correlations", and was answered affirmatively in a breakthrough of Slofstra. We give a new proof of this result by constructing a strikingly simple correlation. In contrast to previous proofs, which involved the representation theory of finitely presented groups and C^*-algebras, our proof is elementary, and leverages one of our self-testing results and a phenomenon known as embezzlement.

PUBLISHED CONTENT AND CONTRIBUTIONS

The chapters of this thesis are based on the following publications or preprints. All papers with multiple authors were the result of a collaborative effort in which each author made significant contributions to all aspects of the paper.

- **Chapter 3.** Section 3.5 is based on: Andrea Coladangelo and Jalex Stark. "Robust self-testing for linear constraint system games". In: *arXiv preprint arXiv:1709.09267* (2017).
- **Chapter 4.** Andrea Coladangelo, Alex B. Grilo, Stacey Jeffery, and Thomas Vidick. "Verifier-on-a-Leash: New Schemes for Verifiable Delegated Quantum Computation, with Quasilinear Resources". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer. (2019), pp. 24777.*
- **Chapter 5.**
  - Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. "All pure bipartite entangled states can be self-tested". In: *Nature communications 8 (2017), p. 15485.*
  - Andrea Coladangelo. "Generalization of the Clauser-Horne-Shimony-Holt inequality self-testing maximally entangled states of any local dimension". In: *Physical Review A 98.5 (2018), p. 052115.*
  - Ivan Šupić, Andrea Coladangelo, Remigiusz Augusiak, and Antonio Acín. "Self-testing multipartite entangled states through projections onto two systems". In: *New Journal of Physics 20 (8), 083041 (2018).*
- **Chapter 6.**
  - Andrea Coladangelo and Jalex Stark. "Unconditional separation of finite and infinite-dimensional quantum correlations". In: *arXiv preprint arXiv:1804.05116* (2018).
  - Andrea Coladangelo. "A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations". In: *arXiv preprint arXiv:1904.02350* (2019).
- **Appendix A.** Andrea Coladangelo. "Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game". In: *Quantum Information & Computation 17.9-10 (2017), pp. 831-865.*

Other works that were completed during my PhD, but are not included in this thesis:

- Andrea Coladangelo and Jalex Stark. "Separation of finite and infinite-dimensional quantum correlations, with infinite question or answer sets". In: *arXiv preprint arXiv:1708.06522* (2017).

- Andrea Coladangelo. "Smart contracts meet quantum cryptography". In: *arXiv preprint arXiv:1902.05214* (2019).

- Andrea Coladangelo and Debbie Leung. "Additive entanglement measures cannot be more than asymptotically continuous". In: *arXiv preprint arXiv:1910.11354* (2019).

- Andrea Coladangelo, Thomas Vidick and Tina Zhang. "Non-interactive zero-knowledge arguments for QMA, with preprocessing". In: *arXiv preprint arXiv:1911.07546* (2019).

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

Chapter 1

INTRODUCTION

Advances in the field of computing have profoundly shaped our society. In recent years, *quantum computing* has received increasing attention as a novel paradigm for computation with the potential to disrupt the current landscape. We expect that quantum computers will achieve dramatic speed-ups for many computational problems. An example of an area that will benefit drastically from these speed-ups is computational chemistry [15], where numerical simulations are employed to understand and predict properties of molecules, and to guide the design of new nanomaterials: quantum computers are expected to be able to efficiently perform simulations that are completely intractable for classical computers. The power of quantum computers can also be leveraged for cryptographic purposes. On the one hand, we know of quantum algorithms that can efficiently factor large numbers [85], a problem whose computational hardness is at the basis of the security of many cryptographic systems in use today: this urges us to redesign our cryptographic systems in a way that is secure against quantum attacks. On the other hand, quantum mechanics can be harnessed to design "unbreakable" cryptographic systems and realize cryptographic tasks that are provably impossible to realize using classical computers alone.

The ongoing race to build a universal quantum computer and realize this potential has fueled remarkable experimental advances. The current setting inevitably raises the following basic question: once we have a universal quantum computer, how do we test that it is functioning correctly? Or more generally, how can a *classical* verifier test any *quantum* device at all? If quantum computers are meant to perform computations and tasks beyond the reach of classical computers, can we hope to verify the outcomes of these computations? The verifier might be an experimentalist with specialized knowledge about a certain experimental setup and the technical equipment involved, or it could be a consumer who has purchased a professed quantum device and has nothing but a laptop and the quantum device itself. There are several possible ways to approach this problem. For example, the experimentalist may attempt to perform a series of measurements on the device, and conduct some statistical analysis on the outcomes by applying techniques from state and process tomography [76] or randomized benchmarking [52]. However, both of these approaches assume that the measurement apparatus is trusted. For the layman consumer, any measurement apparatus is just as untrusted as the quantum device to be tested. For a classical verifier to unequivocally test and certify a quantum system, that system should be modeled in a *device-independent* way, i.e. as a black-box having classical inputs (e.g. measurement settings) and classical outputs (e.g. measurement outcomes).

Bell's theorem [9], a profound discovery in physics published in 1964, provides a partial solution to this problem. It asserts that measurements on spatially isolated quantum systems can produce statistics that are not compatible with any local hidden variable theory (such as Newtonian physics). Such statistics are only possible if the two quantum systems are *entangled*, a characteristically quantum phenomenon that is central to many quantum advantages in computational tasks. The operational consequence of Bell's theorem is that one can design a statistical test to detect the presence of entanglement. Assuming quantum mechanics is correct, this allows a classical verifier to at least certify that her device is exhibiting a genuine quantum behaviour.

Remarkably, it is possible to go beyond merely detecting the presence of entanglement. In some special cases, the measurement statistics can be attained exclusively by a *unique* quantum apparatus (up to some irreducible degrees of freedom). In such cases, a single (a priori very modest) physical assumption about the device to be tested, namely that it consists of two spatially isolated components, allows to characterize the device entirely.

This realization has led to important advances in the field of quantum cryptography, including the first fully device-independent security proofs for quantum key-distribution [96, 64], randomness expansion [64], and delegated quantum computation [82].

The problem of certifying the behaviour of quantum devices is at the heart of this thesis. It is not only compelling from a practical standpoint, but has deep connections to fundamental questions about the nature of entanglement, some of which I hope will be unveiled to the reader of this thesis. It is also a problem that has fascinated me since the start of my PhD: one can think of such a certification procedure (or certificate), whenever it exists, as a "classical fingerprint" of a quantum system, in the sense that the *classical* transcript obtained by the verifier's interaction with the quantum device singles out a unique *quantum* apparatus that is compatible with it. It is not obvious at all that such a certificate should exist, and it is remarkable that it does even in special cases.

1.1 This thesis

Several natural questions arise when thinking about the device-independent certification of quantum devices: does the set of quantum apparatus that can be certified by a classical verifier consist of a few exceptions, or is such a certification a more general phenomenon? If so, can it be exploited not only to certify a fixed quantum apparatus, but to orchestrate a full-fledged quantum computation in a verifiable way? Crucially, it is entanglement that makes these certifications possible at all. Does the answer to these questions yield a more refined understanding of entanglement as a fundamental resource in quantum information? This thesis makes progress on these questions, and provides a resolution to some of them. Before outlining the contents of this thesis, we will informally introduce

the framework in which we study these questions.

1.1.1 The framework: device-independent self-testing

The framework that we work in was first introduced by Bell [9], who at the time was not explicitly concerned with the problem of certifying quantum devices, but rather with exhibiting the non-locality of quantum mechanics. The setup consists of a verifier and her quantum device. The verifier wishes to certify properties of her, a priori uncharacterized, quantum device by interacting classically with it, by probing it with classical questions and expecting classical answers in return. As mentioned earlier, we make just one physical assumption about the system to be tested: that it consists of two spatially isolated components (usually referred to as the players, the provers, or Alice and Bob) that are unable to communicate throughout the experiment. The behaviour of the provers is captured by the joint distribution of their answers as a function of their questions. We refer to this data as a *bipartite correlation*. Formally, a bipartite correlation captures the scenario where there is one round of interaction between the verifier and the provers, but this notion can be generalized naturally to more rounds of interaction. Typically, the two provers are thought of as cooperatively playing a game refereed by the verifier (i.e. they are cooperatively trying to pass the verifier's test), which is traditionally referred to as a *non-local game*. Subject to the constraint that the provers cannot communicate and *do not* share any entanglement (i.e. they are classical), it is possible to efficiently compute a tight upper bound on the expected winning probability of the provers in the game. Such a bound is referred to as a Bell inequality. According to Bell's theorem [9], in some cases, it is possible for provers who share entanglement to *violate* such a bound. This implies that the violation of a Bell inequality can be regarded as a certificate of entanglement.

The area of device-independent self-testing seeks to make even stronger statements about the quantum system under study, by identifying *which measurements* are being performed, and on *which state*. The device-independent approach exploits the fact that certain correlations can be uniquely achieved (up to local isometries) by particular measurements on a particular quantum state. When this is the case, we say that the correlation self-tests the state and the measurements. The term "self-testing", in the context of Bell experiments, was coined by Mayers and Yao [58], and the most famous example of a self-test is given by the CHSH game [17]. In this game, a classical verifier selects uniformly random questions $x, y \in \{0, 1\}$, and sends x to Alice and y to Bob. The players return answers a and b respectively. They win the game if the questions and answers satisfy $a \oplus b = x \cdot y$. It is easy to see that the players win with probability $\frac{3}{4}$ if they always return the answer 0. In fact, a simple convexity argument shows that this is also the best that classical players can do. Surprisingly, players who share entanglement can outperform their classical counterparts, and can win the game with probability as high as $\cos^2(\frac{\pi}{8}) \approx 0.85$! Sharing a maximally entangled pair of qubits (also known as an EPR pair) before the game begins, allows the players to correlate

their answers optimally, and to achieve a winning probability of ≈ 0.85. However, the real *raison d'etre* of this thesis is that $\cos^2(\frac{\pi}{8})$ is a "fingerprint" of an EPR pair: one can show that this is the *unique* state that is compatible with such a winning probability. By observing a winning probability of $\cos^2(\frac{\pi}{8})$, a classical verifier can certify that the quantum device under study contains an EPR pair. Of course, in practice it is not possible to "observe" a correlation, or a winning probability, directly. Rather, one can only repeat the experiment several times and make an estimate with some statistical confidence. It is thus important that the self-testing statement also holds "approximately" [62, 82], meaning that a close-to-optimal winning probability still implies that the underlying state and measurements are close to ideal. This property is often referred to as "robustness".

1.1.2 Outline

In Chapter 2, we cover some preliminary notions, and we give a formal introduction to quantum correlations and non-local games.

In Chapter 3, we introduce the formalism of self-testing, and lay the foundations for much of the work in this thesis. This chapter gives a relatively self-contained introduction to the basics of the theory of self-testing. We start by reviewing the CHSH game, and we provide a (detailed sketch) proof that maximal violation of the CHSH inequality is uniquely attained by an EPR pair. We introduce the concept of a "swap isometry", a technique that is used to extract EPR pairs from states and measurements that satisfy certain natural constraints. We then describe the tilted CHSH inequality, which generalizes the CHSH inequality to partially entangled qubits, and is a building block for later chapters. In the final section of this chapter, we introduce another famous non-local game: the Magic Square game. We take this as an opportunity to introduce a representation-theoretic framework for self-testing, based on an approach developed by Cleve, Liu and Slofstra, and extended in the original work [24]. The framework applies to the Magic Square game and to a wider class of non-local games, known as Linear Constraint System (LCS) games. In an LCS game, questions represent equations from a system of linear equations, and the players' answers are assignments to the variables appearing in the queried equation: the condition for winning the game is that the players' assignments should satisfy their respective equations, and should be consistent with each other (players assign the same value to common variables). In this section, we build up to a general self-testing theorem that applies to a broad class of LCS games. We apply this theorem to deduce that a perfect winning probability in the Magic Square and Magic Pentagram games self-tests two and three EPR pairs respectively.

In Chapter 4, we explore a concrete application of self-testing to the problem of verifiably delegating a quantum computation. We address the following question. How can a classical verifier exploit self-testing results to delegate her computation to a potentially malicious server in a way that allows

her to verify the correctness of the outcome? We will lead up to this question by discussing a necessary ingredient for such a task: the certification of many EPR pairs. Orchestrating a full-fledged quantum computation requires at the very least an amount of resources that scales linearly with the size of the computation. For this reason, it is essential that a classical verifier be able to certify not just one, but many EPR pairs. The most natural way to do this is by repeating a single self-test (say the CHSH game) many times *in sequence*, and requiring that a high-enough fraction of the games be won. A more round-efficient way of doing this is by repeating the CHSH game in parallel, i.e. asking all the questions for many copies of the game simultaneously, and requiring all the answers at once. We start by reviewing the Pauli Braiding test of Natarajan and Vidick [69], which allows to test products of Pauli X and Pauli Z measurements on many EPR pairs, with a robustness that scales independently of the number of EPR pairs tested. Our main technical contribution is to extend the Pauli Braiding test first to include Pauli Y measurements, and subsequently to test any measurement that is a product of single-qubit Clifford observables. Finally, we apply this test to obtain a protocol whereby a classical verifier can verifiably delegate her quantum computation to two spatially isolated provers. The complexity overhead of our protocol for delegating a g-gate quantum circuit scales as $O(g \log g)$. Such a scaling is near optimal (the complexity of the delegation has to be at least $\Omega(g)$), and marks a dramatic improvement over the first scheme by Reichardt, Unger and Vazirani [82], whose overall complexity scaled as $O(g^{8192})$.

Chapter 5 is devoted to one of the main results of this thesis. We address the question of whether self-testing is a property of a few special states, for example EPR pairs, tilted EPR pairs and copies of these, or if such examples are just instances of a more general phenomenon. A number of special cases have been solved over several years, providing examples of states that can be self-tested [102, 7, 83, 103, 101, 75, 60]. These include all partially entangled pairs of qubits, some particular states of qutrits, and a few multipartite states. Hence, while it seems clear that self-testing is not an exclusive characteristic of maximally entangled states nor qubit states, for some time little was known about self-testing higher-dimensional entangled states (i.e. pairs of entangled qudits for $d > 2$). In this chapter, we address this question, and we settle it completely: we show that for any pure bipartite entangled state of any finite local dimension there exists a correlation that self-tests it. In the maximally entangled case, we are also able to extract an explicit family of Bell inequalities whose maximal violation is attained precisely at the self-testing correlation. Such a family generalizes the CHSH inequality to any local dimension, and is the first example of a family of Bell inequalities self-testing the maximally entangled pair of qudits, for any $d \geq 2$. In the final part of the chapter, we move on to the multipartite case, which is mostly unexplored. The main difficulty with multipartite states is that they do not necessarily admit a Schmidt decomposition. As a consequence of this, there exist multipartite states that are not related by a local isometry to their complex conjugate (in some basis). These states cannot possibly be self-tested, in the

traditional sense, since taking the complex conjugate of a state and some measurements leaves the correlation invariant. In this section, we show that any multipartite partially entangled GHZ state can be self-tested, and we use this as a building block to show that any multipartite state of qudits that admits a Schmidt decomposition can be self-tested.

In the final chapter of this thesis, Chapter 6, we draw a connection between the self-testing results discussed so far and basic questions about quantum correlation sets and entanglement. Even though quantum correlations are central objects in the theory of self-testing and throughout quantum information more generally, our understanding of these is far from complete. Several fundamental questions about quantum correlation sets are unanswered. One example is the following: does the set of attainable correlations change if we allow the provers to share infinite-dimensional entanglement, as opposed to just finite-dimensional entanglement? In other words, does there exist a correlation that *requires* infinite-dimensional quantum systems to be attained exactly? One of the main results of this thesis is a resolution of this question: we show that there exists a correlation which is attained exclusively by infinite-dimensional quantum systems. We describe our solution in the first half of the chapter. In the second half, we focus our attention on the problem of certifying high-dimensional entanglement via non-local games. In this context, we do not necessarily seek to characterize exactly the states and measurements of a quantum apparatus. Rather, we are looking to provide a lower bound on the dimension of the quantum system. Thus, the characterization that we seek is less specialized than for a self-testing statement, but we seek a test that is, in some sense, as efficient as possible. To this end, we describe a strikingly simple non-local game with the property that an ϵ-close to optimal strategy requires the players to share an entangled state of dimension at least $2^{\Omega(\frac{1}{poly(\epsilon)})}$. This matches the best known tradeoff between precision and dimension, and it does so via a very simple and direct construction. As a corollary, the existence of such a game gives a new proof of the non-closure of the set of quantum correlations, a recent breakthrough result in quantum information [89]. In contrast to previous proofs, which relied on the representation theory of finitely presented groups and C^*-algebras, ours is elementary, and is based on one of our previous self-testing results and on a phenomenon known as embezzlement.

A few organizational remarks. Starting from Chapter 3, each chapter begins with a few sentences that introduce the topic, followed by a brief overview of the structure of the chapter. Chapters 2 and 3 (except Section 3.5) are essential to the rest of the thesis. Chapter 4 is not needed to understand Chapters 5 and 6. Chapter 5 (excluding Section 5.3) is helpful in understanding Chapter 6, although not strictly essential if one is willing to accept a few results from Chapter 5.

Chapter 2

PRELIMINARIES

2.1 Notation

For an event E, we use 1_E to denote the indicator variable for that event, so $1_E = 1$ if E is true, and $1_E = 0$ otherwise. We write $\mathrm{poly}(\varepsilon)$ for $O(\varepsilon^c)$, where c is a universal constant that may change each time the notation is used. For a positive integer n, we denote by $[n]$ the set $\{1,..,n\}$. δ_{ij} is the Kronecker delta.

For a Hilbert space $\mathcal{H}$, $\mathcal{L}(\mathcal{H})$ is the space of linear operators on $\mathcal{H}$. We denote by $\mathrm{U}(\mathcal{H})$ the set of unitary operators, $\mathrm{Obs}(\mathcal{H})$ the set of binary observables, i.e. self-adjoint operators with ± 1 eigenvalues, $\mathrm{Proj}(\mathcal{H})$ the set of projectors on $\mathcal{H}$, $D(\mathcal{H})$ the set of density operators on $\mathcal{H}$, i.e. positive semi-definite operators with unit trace. For an operator X, we denote its trace by $\mathrm{Tr}[X]$.

Define the Pauli matrices

$$\sigma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \text{and} \qquad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.1}$$

For an operator A, we denote by $A^\dagger$ its adjoint.

We let $|\Phi^+\rangle$ denote an EPR pair:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right).$$

We will sometimes also denote this by $|\mathrm{EPR}\rangle$.

An isometry is a linear map $V : \mathcal{H} \to \mathcal{H}'$ such that $V^\dagger V = I_{\mathcal{H}}$.

By *local isometry* we mean a channel $\Phi : \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{L}(\mathcal{H}'_A \otimes \mathcal{H}'_B)$ which factors as $\Phi(\rho) = (V_A \otimes V_B)\rho(V_A \otimes V_B)^\dagger$, where $V_A : \mathcal{H}_A \to \mathcal{H}'_A, V_B : \mathcal{H}_B \to \mathcal{H}'_B$ are isometries.

For some unitary or isometry $V, \delta > 0$, states $|\psi\rangle, |\phi\rangle$, we write $|\psi\rangle \approx_{V,\delta} |\phi\rangle$ if $\| V|\psi\rangle - |\phi\rangle \| \leq \delta$, where $\| \cdot \|$ is the Euclidean norm. We write $|\psi\rangle \approx_\delta |\phi\rangle$ if $\| |\psi\rangle - |\phi\rangle \| \leq \delta$. We use the same notation for mixed states, except we consider the trace norm $\| \cdot \|_1$, where $\|A\|_1 = \mathrm{Tr}\left[\sqrt{AA^\dagger}\right]$.

For an introduction to the basics of quantum information, we refer the reader to [71] or [81].

2.2 Quantum correlations

Quantum correlations are the fundamental object of study of this thesis. We introduce them formally in this section.

Informally, let Alice and Bob be two non-communicating provers. Consider the scenario in which a verifier sends one question to each prover and receives an answer from each prover. The behaviour of the provers is captured by the joint distribution of their answers as a function of their questions. We refer to this data as a *bipartite correlation*.

Formally, given sets $\mathcal{X}$,$\mathcal{Y}$, $\mathcal{A}$, $\mathcal{B}$, a (bipartite) *correlation* is a collection $\{p(a,b|x,y) : a \in \mathcal{A}, b \in \mathcal{B}\}_{(x,y)\in\mathcal{X}\times\mathcal{Y}}$, where each $p(\cdot,\cdot|x,y)$ is a probability distibution over $\mathcal{A}\times\mathcal{B}$. We interpret the correlation as describing the outcomes of a measurement scenario with two parties, say Alice and Bob. $p(a,b|x,y)$ is the probability that Alice outputs a and Bob outputs b, given that Alice used measurement setting x and Bob used setting y. $\mathcal{X}$ and $\mathcal{Y}$ are referred to as the *question sets*, while $\mathcal{A}$ and $\mathcal{B}$ are referred to as as the *answer sets*.

Given question sets and answer sets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{A}$, $\mathcal{B}$, a *quantum strategy* is specified by Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a state $\rho \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$, and projective measurements $\{\Pi^a_{A_x} : a \in \mathcal{A}\}$ on $\mathcal{H}_A$ for $x \in \mathcal{X}$, and $\{\Pi^b_{B_y} : b \in \mathcal{B}\}$ on $\mathcal{H}_B$ for $y \in \mathcal{Y}$. We say that it *induces correlation* p if

$$p(a,b|x,y) = \mathrm{Tr}\left[\Pi^a_{A_x} \otimes \Pi^b_{B_y} \rho\right] \text{ for all } a \in \mathcal{A}, b \in \mathcal{B}, x \in \mathcal{X}, y \in \mathcal{Y}.$$

Sometimes we refer to a quantum strategy as a triple $\left(\rho, \{\Pi^a_{A_x} : a \in \mathcal{A}\}_{x\in\mathcal{X}}, \{\Pi^b_{B_y} : b \in \mathcal{B}\}_{y\in\mathcal{Y}}\right)$. If we wish to emphasize the underlying Hilbert space, we write $\left(\rho \in D(\mathcal{H}_A \otimes \mathcal{H}_B), \{\Pi^a_{A_x} : a \in \mathcal{A}\}_{x\in\mathcal{X}}, \{\Pi^b_{B_y} : b \in \mathcal{B}\}_{y\in\mathcal{Y}}\right)$. Notice that we have chosen our measurements to be projective. This choice is without loss of generality. The most general measurements are modeled by POVMs, but Naimark's dilation theorem implies that any correlation attained using POVMs can also be attained using projective measurements (possibly of larger dimension). We sometimes describe a quantum strategy by specifying an observable for each question. The observables in turn specify the projectors through their eigenspaces.

A correlation is said to be quantum if there exists a quantum strategy that induces it (we will use the verbs "induce" and "attain" interchangeably). We refine this, and we say that a quantum correlation is *finite-dimensional* (*infinite-dimensional*) if it is induced by a quantum strategy on finite-dimensional (infinite-dimensional and separable) Hilbert spaces. In the rest of this thesis, when we refer to infinite-dimensional Hilbert spaces we always assume that they are separable. We denote by $\mathcal{C}_q^{m,n,r,s}$ and $\mathcal{C}_{qs}^{m,n,r,s}$ respectively the sets of finite and infinite-dimensional quantum correlations on question sets of sizes m,n and answer sets of sizes r,s.

Correlation tables A convenient way to describe correlations is through *correlation tables*. A correlation p on $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{A}$, $\mathcal{B}$ is completely specified by correlation tables T_{xy} for $x \in \mathcal{X}, y \in \mathcal{Y}$, with entries $T_{xy}(a,b) = p(a,b|x,y)$. See Table 2.1 for an example.

a \ b	0	1
0	$p(0,0\|x,y)$	$p(0,1\|x,y)$
1	$p(1,0\|x,y)$	$p(1,1\|x,y)$

Table 2.1: The correlation table on question (x,y) of a correlation on answer sets $\mathcal{A} = \mathcal{B} = \{0,1\}$.

For $\omega \in [0,1]$ and a correlation table T_{xy}, we write $\omega \cdot T_{xy}$ to denote entry-wise multiplication of T_{xy} by ω. We may refer to ω as a *weight*.

2.3 Non-local games

Definition 1. *A non-local game G is a tuple $G = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, D, V)$, where $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$ are sets, D is a distribution over $\mathcal{X} \times \mathcal{Y}$, and $V : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \mathbb{R}$. $\mathcal{X}$ and $\mathcal{Y}$ are referred to as question sets, and $\mathcal{A}$ and $\mathcal{B}$ as answer sets. V is referred to as the scoring function.*

We denote by $D(x,y)$ the probability of outcome x,y according to distribution D. Note that we use the term *non-local game* to refer to games in which the scoring function V can take any real value, not just values in $\{0,1\}$ like is sometimes the case in the literature. With this nomenclature, non-local games and Bell inequalities are equivalent.

Definition 2 (Quantum strategy for a non-local game)**.** *A quantum strategy for a non-local game $G = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, D, V)$ is a triple*

$$\left(\rho \in D(\mathcal{H}_A \otimes \mathcal{H}_B), \{\Pi^a_{A_x} : a \in \mathcal{A}\}_{x\in\mathcal{X}}, \{\Pi^b_{B_y} : b \in \mathcal{B}\}_{y\in\mathcal{Y}}\right),$$

where $\mathcal{H}_A, \mathcal{H}_B$ are Hilbert spaces, $\{\Pi^a_{A_x} : a \in \mathcal{A}\}_{x\in\mathcal{X}}$ is a set of projective measurements on $\mathcal{H}_A$, and $\{\Pi^b_{B_y} : b \in \mathcal{B}\}_{y\in\mathcal{Y}}$ on $\mathcal{H}_B$.

Definition 3 (Value of a quantum strategy in a game)**.** *Let $G = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, D, V)$ be a non-local game, and $S = (|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{\Pi^a_{A_x} : a \in \mathcal{A}\}_{x\in\mathcal{X}}, \{\Pi^b_{B_y} : b \in \mathcal{B}\}_{y\in\mathcal{Y}})$ a quantum strategy for G. The value of S in G is*

$$\omega(S,G) := \sum_{x\in\mathcal{X}, y\in\mathcal{Y}} D(x,y) \cdot V(x,y,a,b) \cdot \mathrm{Tr}\left[\Pi^a_{A_x} \otimes \Pi^b_{B_y} \rho\right].$$

Note that the value $\omega(S,G)$ corresponds to the expected score of strategy S in game G, assuming that questions are distributed according to D, and that the score is determined by the function V.

Definition 4 (Quantum value of a game)**.** *The quantum value* $\omega^*(G)$ *of a game* $G = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, D, V)$ *is defined as follows:*

$$\omega^*(G) := \sup_S \omega(S, G)\,,$$

where the supremum is taken over all quantum strategies for G*.*

Since the closure of the set of finite-dimensional quantum correlations contains the set of infinite-dimensional quantum correlations [84], it does not matter whether the supremum in the definition of ω^* is taken over finite or infinite-dimensional strategies (i.e. whether $\mathcal{H}_A$ and $\mathcal{H}_B$ are finite or infinite-dimensional).

We define the value of a correlation in a game.

Definition 5 (Value of a correlation in a game)**.** *Let* $G = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, D, V)$ *be a non-local game, and* $p = \{p(a, b|x, y) : a \in \mathcal{A}, b \in \mathcal{B}\}_{(x,y)\in\mathcal{X}\times\mathcal{Y}}$ *a correlation. The value* $\omega(p, G)$ *of* p *in* G *is defined as*

$$\omega(p, G) := \sum_{x\in\mathcal{X}, y\in\mathcal{Y}} D(x, y) \cdot V(x, y, a, b) \cdot p(a, b|x, y)\,.$$

Clearly, if p is the correlation induced by a quantum strategy S for game G, then $\omega(p, G) = \omega(S, G)$.

Chapter 3

SELF-TESTING: A REMARKABLE PHENOMENON

The term device-independent self-testing refers to a situation in which the statistics of an interaction between a classical verifier and the two spatially isolated components of a quantum device are sufficient to characterize the state of the device and the measurements in each component. The area of self-testing and its theoretical foundations have developed significantly in recent years. The theory of self-testing has been fruitfully applied to quantum cryptography [96, 64, 82, 27], to the foundations of entanglement and the study of quantum correlation sets [26, 20], and to the study of the complexity of multiprover interactive proofs with entangled provers [70]. In this section, our aim is to give a relatively self-contained introduction to the basics of the theory of self-testing. This will serve as the basis for much of the work in this thesis. For a thorough survey of the self-testing literature, we recommend [93].

Organization In Section 3.1, we define the term self-testing formally in its two variants, from correlations and from non-local games. We define the notion of robust self-testing. In Section 3.2, we formally introduce the CHSH game and the CHSH inequality. We then give a detailed sketch of the proof that maximal violation of the CHSH inequality self-tests an EPR pair. In Section 3.3, we introduce a basic tool, known as the "swap isometry", which plays a role in several of the self-tests appearing in later chapters. In Section 3.4, we introduce the tilted CHSH inequality and its self-testing properties (without proof). In Section 3.5, we introduce a representation-theoretic framework for studying the self-testing properties of Linear Constraint System (LCS) games, like the Magic Square game. We build up to a general self-testing theorem for a broad class of LCS games, which we apply to prove self-testing of the Magic Square and Magic Pentagram games. Section 3.5 is not required to understand the rest of the thesis (although it is helpful to understand our self-test from Chapter 4).

3.1 Definitions

Definition 6 (Self-testing)**.** *We say that a correlation* $\{p^*(a,b|x,y) : a \in \mathcal{A}, b \in \mathcal{B}\}_{x\in\mathcal{X},y\in\mathcal{Y}}$ *self-tests a strategy* $\tilde{S} = \left(|\Psi\rangle\langle\Psi|, \{\tilde{\Pi}^a_{A_x} : a \in \mathcal{A}\}_{x\in\mathcal{X}}, \{\tilde{\Pi}^b_{B_y} : b \in \mathcal{B}\}_{y\in\mathcal{Y}}\right)$ *if, for any strategy* $S = \left(\rho, \{\Pi^a_{A_x} : a \in \mathcal{A}\}_{x\in\mathcal{X}}, \{\Pi^b_{B_y} : b \in \mathcal{B}\}_{y\in\mathcal{Y}}\right)$ *that attains* p^**, there exists a local isometry* $\Phi = \Phi_A \otimes \Phi_B$ *and an auxiliary state* ρ_{extra} *such that, for all* $x \in \mathcal{X}, y \in \mathcal{Y}, a \in \mathcal{A}, b \in \mathcal{B}$*,*

$$\Phi(\rho) = |\Psi\rangle \langle\Psi| \otimes \rho_{extra} \tag{3.1}$$

$$\Phi(\Pi^a_{A_x} \otimes \Pi^b_{B_y} \rho \, \Pi^a_{A_x} \otimes \Pi^b_{B_y}) = \left(\tilde{\Pi}^a_{A_x} \otimes \tilde{\Pi}^b_{B_y} |\Psi\rangle \langle\Psi| \, \tilde{\Pi}^a_{A_x} \otimes \tilde{\Pi}^b_{B_y}\right) \otimes \rho_{extra} \, . \tag{3.2}$$

Sometimes, we refer to *self-testing of the state* when we are only concerned with the guarantee of equation (3.1), and not (3.2). We remark that the reason why we only defined self-testing of a strategy $\tilde{S}$ specified by a pure state is that it is known that mixed states cannot be self-tested according to this definition [86].

In the definition above, one typically assumes that the quantifier is over all *finite-dimensional* strategies S. However, our results in later chapters also hold when quantifying over all possibly infinite-dimensional strategies (on separable Hilbert spaces). This distinction is only of importance for Corollary 7. When proving our self-testing results, we will highlight the parts of the proofs in which this distinction is important.

When a quantum strategy S is approximately related by a local isometry (and tensoring with some auxiliary state) to a strategy $\tilde{S}$, just like the two strategies in equations (3.3) and (3.4), we say that S *is equal to* $\tilde{S}$ *up to local isometry*. Notice that such a relation is not symmetric (the state in S could be tensored with a lot of entanglement which is not actually used, and would result in a very entangled ρ_{extra}).

We can similarly define self-testing for non-local games.

Definition 7 (Self-testing for non-local games)**.** *We say that a non-local game* G self-tests *a quantum strategy* $\tilde{S}$ *if any quantum strategy* S *that achieves the quantum value* $w^*(G)$ *is equal to* $\tilde{S}$ *up to local isometry.*

Remark 1. Notice that self-testing from a non-local game (as in Definition 7) implies self-testing via a correlation (as in Definition 6). This is because the correlation induced by strategy $\tilde{S}$ in Definition 7 clearly also self-tests $\tilde{S}$ according to Definition 6. The reverse is not necessarily true. It is not clear that for any correlation p^* that self-tests some strategy $\tilde{S}$ according to Definition 6, there exists a non-local game whose entangled value is attained precisely at p^*. In fact, we know of explicit counterexamples in which this reverse implication does not hold [41].

Robust self-testing

In practice, probabilities cannot be estimated exactly, but only approximately up to some statistical error. In order for self-testing results to be useful in practice, it is essential that they be *robust*: a close-to-ideal correlation should certify a close-to-ideal strategy. We first define a notion of distance between two correlations.

Definition 8. *(Distance between correlations) Let* $\{p(a,b|x,y) : (a,b) \in \mathcal{A}\times\mathcal{B}\}_{(x,y)\in\mathcal{X}\times\mathcal{Y}}$ *and* $\{p'(a,b|x,y) : (a,b) \in \mathcal{A}\times\mathcal{B}\}_{(x,y)\in\mathcal{X}\times\mathcal{Y}}$ *be correlations on the same question and answer sets* $\mathcal{X},\mathcal{Y},\mathcal{A},\mathcal{B}$*. Define their distance* $|\cdot|_{corr}$ *as*

$$|p-p'|_{corr} := \sup_{x,y}\sum_{a,b}|p(a,b|x,y)-p'(a,b|x,y)|\,.$$

Definition 9 (Robust self-testing)**.** *We say that a correlation* $\{p^*(a,b|x,y) : a\in\mathcal{A}, b\in\mathcal{B}\}_{x\in\mathcal{X},y\in\mathcal{Y}}$ *self-tests a strategy* $\tilde{S} = \left(|\Psi\rangle\langle\Psi|, \{\tilde{\Pi}^a_{A_x} : a\in\mathcal{A}\}_{x\in\mathcal{X}}, \{\tilde{\Pi}^b_{B_y} : b\in\mathcal{B}\}_{y\in\mathcal{Y}}\right)$ *with robustness* δ*, where* $\delta(\epsilon)\to 0$*, as* $\epsilon\to 0$*, if for any strategy* $S = \left(\rho, \{\Pi^a_{A_x} : a\in\mathcal{A}\}_{x\in\mathcal{X}}, \{\Pi^b_{B_y} : b\in\mathcal{B}\}_{y\in\mathcal{Y}}\right)$ *inducing a correlation* p *such that* $|p-p^*|_{corr}\leq\epsilon$*, there exists a local isometry* $\Phi = \Phi_A\otimes\Phi_B$*, and an auxiliary state* ρ_{extra} *such that, for all* $x\in\mathcal{X}, y\in\mathcal{Y}, a\in\mathcal{A}, b\in\mathcal{B}$*,*

$$\Phi(\rho) \approx_{\delta^2(\epsilon)} |\Psi\rangle\langle\Psi|\otimes\rho_{extra} \tag{3.3}$$

$$\Phi(\Pi^a_{A_x}\otimes\Pi^b_{B_y}\,\rho\,\Pi^a_{A_x}\otimes\Pi^b_{B_y}) \approx_{\delta^2(\epsilon)} \left(\tilde{\Pi}^a_{A_x}\otimes\tilde{\Pi}^b_{B_y}|\Psi\rangle\langle\Psi|\tilde{\Pi}^a_{A_x}\otimes\tilde{\Pi}^b_{B_y}\right)\otimes\rho_{extra}\,. \tag{3.4}$$

Notice that the distance is $\delta^2(\epsilon)$ in (3.3) and (3.4) rather than the more natural $\delta(\epsilon)$. This is just a convention that we pick so that the distance is $\delta(\epsilon)$ when comparing Euclidean norms.

When a quantum strategy S is approximately related by a local isometry (and tensoring with some auxiliary state) to a strategy $\tilde{S}$, just like the two strategies in equations (3.3) and (3.4), we say that S *is* $\delta(\epsilon)$*-approximately equal to* $\tilde{S}$ *up to local isometry*.

The definition of robust self-testing for non-local games is similar.

Definition 10 (Robust self-testing for non-local games)**.** *We say that a non-local game* G *self-tests a quantum strategy* $\tilde{S}$ *with robustness* δ*, where* $\delta(\epsilon)\to 0$*, as* $\epsilon\to 0$*, if for any strategy* S *such that* $w(S,G) > w^*(G)-\epsilon$*, it holds that* S *is* $\delta(\epsilon)$*-approximately equal to* $\tilde{S}$ *up to local isometry.*

Remark 2. In the rest of this thesis, when we fix an arbitrary quantum strategy, we will often restrict ourselves to strategies that consist of a pure state. In most cases this is without loss of generality, since any correlation that is attained by a mixed state can be attained exactly by considering a purification (on a system of possibly larger dimension). This is the case for example in Chapters

4 and 6, where the end goal is not to prove a self-testing result, but rather self-testing is used as a tool (to achieve a delegated quantum computation protocol in Chapter 4 and to prove separation of certain quantum correlation sets in Chapter 6). In the case of Chapter 5, however, this restriction is not without loss of generality because what we prove is a self-testing result according to definition 6 (and it is not clear a priori if the restriction to pure states is without loss of generality). In this case, the restriction that we make is for notational convenience, but it will be apparent from the proofs that the same arguments go through virtually unchanged when one allows for strategies consisting of mixed states.

3.2 The CHSH game

The CHSH game is the simplest example of a non-local game. It was discovered in 1969 by Clauser, Horne, Shimony, and Holt [17], and it is the most famous witness of Bell's theorem [9].

In the CHSH game, Alice and Bob receive single-bit questions x and y respectively, sampled uniformly at random, and return single-bit answers a and b respectively. So $\mathcal{X} = \mathcal{Y} = \mathcal{A} = \mathcal{B} = \{0,1\}$. Alice and Bob win the game if $a \oplus b = x \cdot y$. It is well-known that the optimal winning probability of any strategy that does not use entanglement is $\frac{3}{4}$. The two players can achieve this by always answering 0. It is not difficult to show that this is also optimal: by a convexity argument, it suffices to consider deterministic strategies of Alice and Bob. One can enumerate them all, and see that each deterministic strategy must fail on at least one question pair.

When the players are allowed to share entanglement, they are able to surpass this classical bound, and win with probability up to $\cos^2(\frac{\pi}{8}) \approx 0.85$. A strategy that achieves this is the following:

Definition 11 (Ideal strategy for CHSH)**.** *The ideal strategy for CHSH consists of the joint state* $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *and observables* A_0, A_1 *and* B_0, B_1 *with* $A_0 = \sigma^z$, $A_1 = \sigma^x$, $B_0 = \frac{\sigma_Z + \sigma_X}{\sqrt{2}}$ *and* $B_1 = \frac{\sigma_Z - \sigma_X}{\sqrt{2}}$. *For each observable, we associate the projection onto the* $+1$*-eigenspace with answer* 0 *and the projection onto the* -1*-eigenspace with answer* 1.

The CHSH inequality

The winning probability in the CHSH game is equivalently captured by the following operator:

$$\hat{S} := A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1 \,, \tag{3.5}$$

where the A_x and B_y are respectively Alice and Bob's observables in the game. For a joint state $|\psi\rangle$ of Alice and Bob, it is easy to check that $\langle\psi|\,\hat{S}\,|\psi\rangle = 4 \cdot (\Pr[\text{Alice and Bob win CHSH}] - \Pr[\text{Alice and Bob lose CHSH}])$. The upper bound of $\frac{3}{4}$ on the winning probability for classical players translates to:

$$\langle\psi|\,\hat{S}\,|\psi\rangle \leq 2\,, \tag{3.6}$$

for any product state $|\psi\rangle$. The upper bound of $\cos^2(\frac{\pi}{8}) = \frac{2+\sqrt{2}}{4}$ translates to:

$$\langle\psi|\,\hat{S}\,|\psi\rangle \leq 2\sqrt{2}\,. \tag{3.7}$$

One can verify that this upper bound is attained by the strategy of Definition 11. We say that this strategy attains the *maximal quantum violation* of the CHSH inequality (3.6).

Inequalities of the kind of (3.6), which separate classical from quantum behaviour are referred to as *Bell inequalities*, and $\hat{S}$ is referred to as a *Bell operator*. Notice that $\hat{S}$ is a linear functional in the probabilities $p(a,b|x,y)$, and thus defines a family of hyperplanes in the space of quantum correlations for the given question and answer set sizes. The hyperplane corresponding to $\hat{S} = 2\sqrt{2}$ is tangent to the quantum correlation set $\mathcal{C}_q^{2,2,2,2}$ at a correlation whose value in the game is optimal.

The bound from (3.7) is also known as Tsirelson's bound. We give a proof of it here.

Theorem 1 (Tsirelson's bound)**.** *Consider any bipartite state $|\psi\rangle$ and binary observables A_0, A_1 on the first tensor factor and B_0, B_1 on the second. Let $\hat{S}$ be defined as in* (3.5)*. Then $\langle\psi|\,\hat{S}\,|\psi\rangle \leq 2\sqrt{2}$.*

Proof. We prove the claim by giving an upper bound on the largest eigenvalue of $\hat{S}$, i.e. $||\hat{S}||_\infty$. Since the A_x and B_y are Hermitian with ± 1 eigenvalues by construction, we have $||A_x||_\infty = ||B_y||_\infty = 1$ and $A_x^2 = \mathbb{1}_{d_A}$ and $B_y^2 = \mathbb{1}_{d_B}$, where the dimensions d_A and d_B of the Hilbert spaces are left unspecified, and may be infinite. The easiest way to obtain the bound is to consider the square of $\hat{S}$, which one can verify to be:

$$\hat{S}^2 \;=\; 4\,\mathbb{1}\otimes\mathbb{1} \;-\; [A_0, A_1]\otimes[B_0, B_1]\,.$$

Finally, we observe that

$$||[A_0, A_1]||_\infty = ||A_0A_1 - A_1A_0||_\infty \;\leq\; ||A_0A_1||_\infty + ||A_1A_0||_\infty \;\leq 2||A_0||_\infty\,||A_1||_\infty \;=\; 2\,, \tag{3.8}$$

where the last inequality uses $|xy| \leq |x|\,|y|$. Similarly, we get $||[B_0, B_1]||_\infty \leq 2$. Therefore $||\hat{S}^2||_\infty \leq 8$, which proves the claim. □

Given that the ideal strategy from Definition 11 attains Tsirelson's bound, we conclude that this bound is tight.

CHSH self-tests an EPR pair

We are now ready to discuss the very first self-testing result of this thesis, which dates back to a work of Summers and Werner [92] and Popescu and Rohrlich [80]: not only does the ideal strategy from

Definition 11 attain maximal violation of the CHSH inequality (or equivalently optimal winning probability in the CHSH game), but it is also the *unique* strategy to do so, up to a degree of freedom of applying a local isometry. In other words, maximal violation of the CHSH inequality self-tests an EPR pair.

Theorem 2 (CHSH self-test)**.** *The CHSH game self-tests the ideal strategy of Definition 11 with robustness* $O(\sqrt{\epsilon})$.

We give a detailed sketch of the proof of Theorem 2. For fully detailed proofs, we refer the reader to either [62] or [82]. Even though they share some common ground, the two proofs are somewhat different in flavour, and each contains worthwhile intuition. Our proof is closer to the latter.

Detailed proof sketch. Let $(|\psi\rangle, \{A_x\}, \{B_y\})$ be a quantum strategy attaining maximal violation of the CHSH inequality. In order to prove Theorem 2, according to Definition 7, we need to exhibit a local isometry Φ such that $\Phi(|\psi\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |extra\rangle$ for some auxiliary state $|extra\rangle$, and similar statements involving the observables A_x, B_y.

From the proof of Tsirelson's bound, we already know that any quantum strategy that maximally violates the CHSH inequality must saturate inequality (3.8). Hence, it must be $||[A_0, A_1]||_\infty = 2$. It is not difficult to see that the saturation of the triangle inequality in (3.8) implies that for any state $|\psi\rangle$ that attains maximal violation, it must hold that $[A_0, A_1]|\psi\rangle = \pm 2A_0A_1|\psi\rangle$. This implies that $\{A_0, A_1\}|\psi\rangle = 0$, i.e. A_0 and A_1 anti-commute when acting on $|\psi\rangle$. Similarly, we obtain $\{B_0, B_1\}|\psi\rangle = 0$. We can now invoke Jordan's Lemma, a tool that is quite frequently used in quantum information, and which allows us to reduce the analysis to the qubit case. For this part of the argument, we assume for simplicity that Alice and Bob's Hilbert spaces are finite-dimensional (although we do not assume any other bound on the dimension). This is required in order to apply Jordan's Lemma. For the full details of the argument for arbitrary Hilbert spaces, which is technical and does not provide particular additional insight, we refer the reader to [82]. Jordan's Lemma states the following:

Lemma 1 (Jordan)**.** *Let* $\hat{A}_0$ *and* $\hat{A}_1$ *be two Hermitian operators on a finite-dimensional Hilbert space with eigenvalues* -1 *and* $+1$*. There exist a basis in which both operators are block-diagonal, in blocks of dimension* 2×2 *at most.*

Applying Jordan's Lemma to both Alice and Bob's Hilbert space allows us to decompose the joint Hilbert space (of a priori unknown dimension) of $|\psi\rangle$ into blocks of dimension 2×2 (i.e. a qubit on Alice tensor a qubit on Bob), 2×1, 1×2 and 1×1. Formally, in an appropriate basis, we can

write: $A_x = \bigoplus_i A_x^{(i)}$, $B_y = \bigoplus_j B_y^{(j)}$, and

$$|\psi\rangle = \bigoplus_{ij} \alpha_{ij} \left|\psi^{(ij)}\right\rangle,$$

Then,

$$\langle\psi| \hat{S} |\psi\rangle = \sum_{ij} |\alpha_{ij}|^2 \left\langle\psi^{(ij)}\right| \hat{S}^{(ij)} \left|\psi^{(ij)}\right\rangle,$$

where $\hat{S}^{(ij)} = A_0^{(i)} \otimes B_0^{(j)} + A_0^{(i)} \otimes B_1^{(j)} + A_1^{(i)} \otimes B_0^{(j)} - A_1^{(i)} \otimes B_1^{(j)}$.

In order to achieve the maximal expected value of $\hat{S}$, the CHSH operator in each block has to be maximized. This implies that each $\left|\psi^{(ij)}\right\rangle$, such that $\alpha_{ij} \neq 0$, has Schmidt rank 2. In particular, there are no 1×2, 2×1 or 1×1 blocks, except corresponding to pairs i, j with $\alpha_{ij} = 0$.

Furthermore, earlier we deduced that $\{A_0, A_1\} |\psi\rangle = 0$ and $\{B_0, B_1\} |\psi\rangle = 0$. This implies that it must be $\{A_0^{(i)}, A_1^{(i)}\} \left|\psi^{(ij)}\right\rangle = 0$ and $\{B_0^{(j)}, B_1^{(j)}\} \left|\psi^{(ij)}\right\rangle = 0$ for all i, j with $\alpha_{ij} \neq 0$. Since both the $A_x^{(i)}$'s and the $B_y^{(j)}$'s are 2×2 matrices, and $\left|\psi^{(ij)}\right\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ has Schmidt rank 2, then it is straightforward to see that it must be $\{A_0^{(i)}, A_1^{(i)}\} = 0$ and $\{B_0^{(j)}, B_1^{(j)}\} = 0$ for all i, j with $\alpha_{ij} \neq 0$ (without the restriction of the operators acting on the state).

Since there is, up to unitary equivalence, a unique two-dimensional representation of the single-qubit Pauli group (i.e. the group generated by σ_Z and σ_X), we deduce that, up to a local change of basis, $A_0^{(i)} = \sigma_Z$, $A_1^{(i)} = \sigma_X$ and $B_0^{(j)} = \sigma_Z$, $B_1^{(j)} = \sigma_X$ for all i, j with $\alpha_{ij} \neq 0$.

We are now able to explicitly write the CHSH operator $\hat{S}^{(ij)}$ for the ij block in this basis as:

$$\sigma_Z \otimes \sigma_Z + \sigma_Z \otimes \sigma_X + \sigma_X \otimes \sigma_Z - \sigma_X \otimes \sigma_X.$$

Since this is just a 2 qubit operator, we can directly compute the (normalized) eigenvector corresponding to the largest eigenvalue. This is:

$$\frac{1}{\sqrt{2}} |0\rangle \left|\psi^+\right\rangle + \frac{1}{\sqrt{2}} |1\rangle \left|\psi^-\right\rangle$$

where $|\psi^+\rangle$ and $|\psi^-\rangle$ are respectively the $+1$ and -1 (unit) eigenvectors of $\frac{\sigma_Z + \sigma_X}{\sqrt{2}}$. In addition, one can check that $\frac{\sigma_Z - \sigma_X}{\sqrt{2}} |\psi^+\rangle = |\psi^-\rangle$ and $\frac{\sigma_Z - \sigma_X}{\sqrt{2}} |\psi^-\rangle = |\psi^+\rangle$.

It is easy to check, then, that one can pick a local unitary $\Phi^{(ij)}$ such that

$$\begin{aligned}
\Phi^{(ij)}\left(\left|\psi^{(ij)}\right\rangle\right) &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
\Phi^{(ij)}(A_0^{(i)} \otimes I) &= \sigma_Z \otimes I \\
\Phi^{(ij)}(A_1^{(i)} \otimes I) &= \sigma_X \otimes I \\
\Phi^{(ij)}(I \otimes B_0^{(j)}) &= I \otimes \frac{\sigma_Z + \sigma_X}{\sqrt{2}} \\
\Phi^{(ij)}(I \otimes B_1^{(j)}) &= I \otimes \frac{\sigma_Z - \sigma_X}{\sqrt{2}}\,.
\end{aligned}$$

The desired self-testing local isometry is $\Phi = \bigoplus_{ij:\alpha_{ij}\neq 0} \Phi^{(ij)} \oplus I$ (up to the natural local isomorphism $\bigoplus_{ij} \mathbb{C}^2 \otimes \mathbb{C}^2 \simeq (\mathbb{C}^2 \otimes \mathbb{C}^2) \otimes \mathbb{C}^k$, where k is the number of blocks, and where we assume that blocks of size 1 are trivially extended to blocks of size 2). □

3.3 The "swap" isometry

In this section, we introduce a basic tool which we refer to as the *swap isometry*. This tool comes in the form of a theorem giving sufficient conditions, in terms of binary observables on Alice and Bob's side, for the existence of an isometry that "extracts" an EPR pair. We will first state the theorem, then explain the intuition behind it, and finally provide a proof. This section is adapted in large part from [62].

Theorem 3. *Suppose that there exists a bipartite state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, binary observables X_A, Z_A on $\mathcal{H}_A$ and X_B, Z_B on $\mathcal{H}_B$ such that:*

$$X_A Z_A |\psi\rangle = -Z_A X_A |\psi\rangle \tag{3.9}$$
$$X_B Z_B |\psi\rangle = -Z_B X_B |\psi\rangle \tag{3.10}$$
$$X_A |\psi\rangle = X_B |\psi\rangle \tag{3.11}$$
$$Z_A |\psi\rangle = Z_B |\psi\rangle\ . \tag{3.12}$$

Then there exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$ and a state $|extra\rangle_{AB}$ such that

$$\Phi(M_A N_B |\psi\rangle) = |extra\rangle_{AB} \otimes (\sigma_M) \otimes \sigma_N) \left|\phi^+\right\rangle_{A'B'}$$

for $M, N \in \{I, X, Z\}$.

Let the SWAP gate be the two-qubit gate the swaps the content of the qubit registers. The intuition behind Theorem 3 is the following: from conditions (3.9)-(3.12), the operators X_A,Z_A, X_B, Z_B act on $|\psi\rangle$ in the same way as $\sigma_X \otimes I$, $\sigma_Z \otimes I$, $I \otimes \sigma_X$, $I \otimes \sigma_Z$ act on the EPR pair. The idea of the

swap isometry is the following: if the uncharacterized operators were exactly the Pauli operators, and $|\psi\rangle$ was indeed the EPR pair, then one could add two ancilla qubits in the state $|00\rangle_{A'B'}$, apply the gate $\mathsf{SWAP}_{AA'} \otimes \mathsf{SWAP}_{BB'}$, and (trivially) obtain the state $|00\rangle_{AB} \otimes (\sigma_M \otimes \sigma_N) |\phi^+\rangle_{A'B'}$. Such a circuit is depicted in Fig. 3.1. The idea of the proof of Theorem 3 is to build the desired

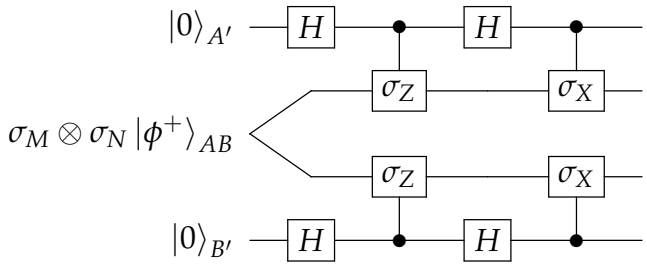


Figure 3.1: A true SWAP gate. Here $M, N \in \{I, X, Z\}$.

isometry Φ by replacing $\sigma_M \otimes \sigma_N |\phi^+\rangle_{AB}$ with $M_A \otimes N_B |\psi\rangle$, and replacing the real σ_Z and σ_X on register A with Z_A and X_A, and replacing the real σ_Z and σ_X on B with Z_B and X_B. The hope is that the constraints (3.9)-(3.12) are enough to capture the essence of the real operators and state. We show that this intuition magically works.

Proof. The isometry is constructed as in figure 3.2. For the case where $M = N = I$, the isometry

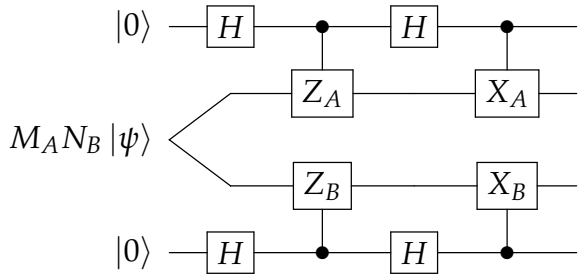


Figure 3.2: Local isometry Φ, where $M, N \in \{I, X, Z\}$.

gives

$$\begin{aligned}
\Phi(|\psi\rangle) &= \frac{1}{4}(I + Z_A)(I + Z_B) |\psi\rangle |00\rangle \\
&+ \frac{1}{4} X_B (I + Z_A)(I - Z_B) |\psi\rangle |01\rangle \\
&+ \frac{1}{4} X_A (I - Z_A)(I + Z_B) |\psi\rangle |10\rangle \\
&+ \frac{1}{4} X_A X_B (I - Z_A)(I - Z_B) |\psi'\rangle |11\rangle .
\end{aligned}$$

Now, for the "11" term, for example, one can use equations (3.9), (3.10) and (3.11) to deduce that $\frac{1}{4}X_AX_B(I-Z_A)(I-Z_B)\,|\psi\rangle\,|11\rangle = \frac{1}{4}(I+Z_A)(I+Z_B)\,|\psi\rangle\,|11\rangle$. For the "01" and "10" terms, one can apply (3.12) and deduce that these terms vanish. All in all, we obtain

$$\Phi(|\psi\rangle) = |extra\rangle\,|\phi^+\rangle\ ,$$

where $|extra\rangle = \frac{(I+Z_A)(I+Z_B)}{\sqrt{2}}\,|\psi\rangle$. The other cases are similar. □

It is not difficult to prove an "approximate" version of Theorem 3 which holds when (3.9)-(3.12) hold ϵ-approximately, and guarantees that the final output is $O(\sqrt{\epsilon})$-close to an EPR pair. Such a calculation can be found in [62]. There, a robust version of Theorem 3 is used to prove that CHSH robustly self-tests the ideal strategy from Definition 11 with $O(\sqrt{\epsilon})$ robustness. The strategy of the proof is to construct, from the observables used by the provers, operators X_A, Z_A, X_B, Z_B satisfying the hypothesis of Theorem 3. On Alice's side, one sets $Z_A = A_0$ and $X_A = A_1$. Notice that we already know that these commute from our proof outline for Theorem 2 (this was a consequence of the saturation of Tsirelson's bound). On Bob's side, we cannot mirror Alice because this would not satisfy (3.11) and (3.12). One instead defines $Z_B = (B_0+B_1)|B_0+B_1|^{-1}$ and $X_B = (B_0-B_1)|B_0-B_1|^{-1}$, where $|X| = \sqrt{XX^\dagger}$. This step is necessary in order to "unitarize" $B_0 \pm B_1$, which a priori need not be unitary. Formally, if B_0+B_1 is not invertible, we first add an identity on the kernel of B_0+B_1, to obtain $B_0+B_1+\mathbb{1}_{\mathrm{Ker}(B_0+B_1)}$, where $\mathbb{1}_{\mathrm{Ker}(B_0+B_1)}$ is the projection on $\mathrm{Ker}(B_0+B_1)$. One can verify that this does not affect the action on $|\psi\rangle$ if the strategy maximally violates CHSH. Then, we take a polar decomposition of $B_0+B_1+\mathbb{1}_{\mathrm{Ker}(B_0+B_1)}$: let U, Π be respectively a unitary and a positive-definite operator such that

$$B_0+B_1+\mathbb{1}_{\mathrm{Ker}(B_0+B_1)} = U\Pi.$$

Then, we define $Z_B = U$. Similarly for X_B.

It is not hard to prove that Z_B and X_B as defined anticommute (notice that $B_0 \pm B_1$ already anti-commute exactly). With more calculations, one can establish conditions (3.11) and (3.12) (we refer to [62] for more details).

3.4 The tilted CHSH inequality

The CHSH inequality can be generalized to a one-parameter family of inequalities which allow to self-test any partially entangled pair of qubits. Such a generalization was discovered by Acín, Massar and Pironio [1], and is a building block for several of the correlations that appear in this work. Given a real parameter $\beta \in [0,2]$, for a product state $|\phi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$, the following holds:

$$\langle\phi\,|\,\beta A_0 + A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1\,|\,\phi\rangle \leq 2+\beta\,.$$

For entangled $|\psi\rangle$, we have instead:

$$\langle\psi\,|\,\beta A_0 + A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1\,|\,\psi\rangle \leq \sqrt{8+2\beta^2}\,. \tag{3.14}$$

The maximum in the tilted CHSH inequality is attained by the following strategy:

Definition 12 (Ideal strategy for tilted CHSH)**.** *Given parameter β, let* $\sin 2\theta = \sqrt{\frac{4-\beta^2}{4+\beta^2}}$, $\mu = \arctan\sin 2\theta$, *and* $\alpha = \tan\theta$. *Define the* α-tilted Pauli operators *as*

$$\sigma_\alpha^z := \cos\mu\sigma^z + \sin\mu\sigma^x, \text{ and } \sigma_\alpha^x := \cos\mu\sigma^z - \sin\mu\sigma^x\,.$$

The ideal strategy for tilted CHSH with parameter β (i.e. achieving maximal violation of (3.14)*) consists of the joint state $|\Psi\rangle = \cos\theta(|00\rangle + \alpha\,|11\rangle)$ and observables A_0, A_1 and B_0, B_1 with $A_0 = \sigma^z$, $A_1 = \sigma^x$, $B_0 = \sigma_\alpha^z$ and $B_1 = \sigma_\alpha^x$. For each observable, we associate the projection onto the $+1$-eigenspace with answer 0 and the projection onto the -1-eigenspace with answer 1.*

We will refer to the tilted CHSH inequality that self-tests the state $|\Psi\rangle = \cos\theta(|00\rangle + \alpha\,|11\rangle)$ as "tilted CHSH for ratio α", as this will be the parameter of interest in later sections, rather than β.

We will state, without proof, the following property of the tilted CHSH inequality.

Lemma 2 ([7])**.** *The tilted CHSH correlation for ratio α self-tests the strategy of Definition 12 with $O(\sqrt{\epsilon})$-robustness.*

We refer the reader to [7] for the proof.

In Chapter 5, we will need the following technical lemma about quantum strategies which achieve maximal violation of the tilted CHSH inequality. This establishes that, from the observables of the strategy, one can construct unitary operators which behave like Pauli X and Pauli Z's when acting on the ideal state. The conditions that such unitary operators satisfy are a generalization of the conditions from Theorem 3. This lemma is a consequence of the analysis of [7].

Lemma 3. *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{B}$. Let A_0, A_1 and B_0, B_1 be binary observables, respectively on $\mathcal{H}_A$ and $\mathcal{H}_B$, with ± 1 eigenvalues. Suppose that*

$$\langle\psi|\,\beta A_0 + A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1\,|\psi\rangle = \sqrt{8+\beta^2}$$

Let $\theta, \mu \in (0, \frac{\pi}{2})$ be such that $\sin 2\theta = \sqrt{\frac{4-\beta^2}{4+\beta^2}}$ *and* $\mu = \arctan\sin 2\theta$. *Then, let $Z_A = A_0$, $X_A = A_1$. Let $B_0 + B_1 + \mathbb{1}_{\mathrm{Ker}(B_0+B_1)} = U^+\Pi^+$ and $B_0 - B_1 + \mathbb{1}_{\mathrm{Ker}(B_0-B_1)} = U^-\Pi^-$ be*

polar decompositions, where $U^{\pm}$ are unitaries and $\Pi^{\pm}$ are positive-definite. Let $Z_B = U^{+}$ and $X_B = U^{-}$. Then, we have

$$Z_A |\psi\rangle = Z_B |\psi\rangle$$
$$\cos\theta X_A(\mathbb{1} - Z_A) |\psi\rangle = \sin\theta X_B(\mathbb{1} + Z_A) |\psi\rangle$$

Parallel self-testing For practical applications, like the one we will explore in Chapter 4, where a classical verifier wishes to delegate a quantum computation to two potentially untrusted quantum servers, it is not enough to test a single EPR pair. If g is the size of the computation (as measured in terms of the number of gates), then the verifier likely needs a quantum device of size at least $\Omega(g)$, say $\Omega(g)$ EPR pairs, and she should be able to certify measurements on a tensor product of these EPR pairs. Such a certification could be performed by sequential repetition, or in parallel, where the verifier asks all of her questions at once, and receives each player's answers all at once. The main technical obstacle in such a setting, is that the players can always induce arbitrary correlations between different copies of the game. Concretely, this obstacle translates into the difficulty of establishing a tensor product structure in the players' a priori unstructured registers.

For the cases of CHSH and tilted CHSH, one can obtain self-testing theorems for a direct correlation-based parallel repetition of these games, based on the original work [22]. The ideas in the proofs expand on some of the concepts discussed here, like the swap isometry, and can be useful to the reader interested in familiarizing with the concepts in this section. We leave a formal description of these results and their proofs in Appendix A.

3.5 A representation-theoretic point of view: the Magic Square game

We conclude this chapter by reviewing another famous non-local game: the Magic Square game [63] (and the qualitatively similar, but less well-known, Magic Pentagram game). Unlike the CHSH game, the Magic Square game has perfect completeness, meaning that there exists a quantum strategy that wins the game with probability 1, while the best classical strategy wins with probability $\frac{8}{9}$. The magic square game belongs to a class of non-local games known as Linear Constraint System (LCS) games. Because of their clean algebraic structure, the Magic Square game, and LCS games more generally, can be studied fruitfully via a representation-theoretic approach. In this section, we outline the representation-theoretic framework for LCS games developed by Cleve, Liu and Slofstra [18]. We extend this framework following our original work [24], where we obtain a general self-testing theorem which applies to a broad class of LCS games. Applying this to the Magic Square game yields a proof that the latter self-tests two EPR pairs, and applying it to the Magic Pentagram game yields a proof that the latter self-tests three EPR pairs. In this section, we only describe and prove the exact version of this self-testing theorem (Theorem 18). Most of the

work, however, goes into obtaining an approximate version of this theorem, but is not included in this thesis. Nonetheless, we elected to include a review of the representation-theoretic framework in this chapter, as we believe it provides an enlightening, and more abstract, perspective on self-testing. The content of this section is helpful, but certainly not essential, to understand the proof of the robust parallel self-testing theorem from Chapter 4, and is not otherwise required for any other section of the main text.

Magic Squares and Pentagrams In [79, 63], Mermin and Peres discovered an algebraic coincidence related to the 3×3 "Magic Square" of operators on $\mathbb{C}^2 \otimes \mathbb{C}^2$ in Figure 3.3.

If we pick any row and take the product of the three operators in that row (note that they commute, so the order does not matter), we get the identity operator. Similarly, we can try this with the columns. Two of the columns give identity while the other gives -1 times identity. Thus, the product of these nine operators depends on whether they are multiplied row by row or column by column. This can be exploited to define a non-local game known as the Mermin–Peres Magic Square game [5] (see Definition 22 and Figure 3.7 for a formal definition). Informally, the Mermin–Peres Magic Square game mod 2 is as follows. The players claim to have a 3×3 square of numbers in which each row and each of the first two columns sums to $0 \pmod 2$, while the third column sums to $1 \pmod 2$. The referee asks the first player to present a row of the supposed square and the second to present a column. They reply respectively with the 3 entries of that row and column in $\{0, 1\}$. They win if their responses sum to 0 or 1 as appropriate, and they give the same number for the entry where the row and column overlap. This game can be won with probability 1 by provers that share two pairs of maximally entangled qubits of dimension 2, but provers with no entanglement can win with probability at most $\frac{8}{9}$. Games which are won in the classical case with probability < 1 but are won in the quantum case with probability 1 are known as *pseudotelepathy games*.

How special is this "algebraic coincidence" and the corresponding game? Arkhipov [6] gives a partial answer to this question by introducing the framework of *magic games*. Starting from any finite graph, one can construct a magic game similar to the Magic Square game. Arkhipov finds that there are exactly two interesting such magic games: the Magic Square (derived from $K_{3,3}$, the complete bipartite graph with parts of size 3) and the Magic Pentagram (derived from K_5, the complete graph on 5 vertices).

Linear Constraint System (LCS) games Linear Constraint System games (hereafter referred to as *LCS games* were introduced by Cleve and Mittal [19], and can be thought of as a generalization of Arkhipov's magic games from graphs to hypergraphs (a connection that we will explain shortly). In an LCS games, questions represent equations from a system of linear equations modulo d, for some $d \in \mathbb{Z}$, and answers correspond to assignments to all variables in the equation. Alice and Bob

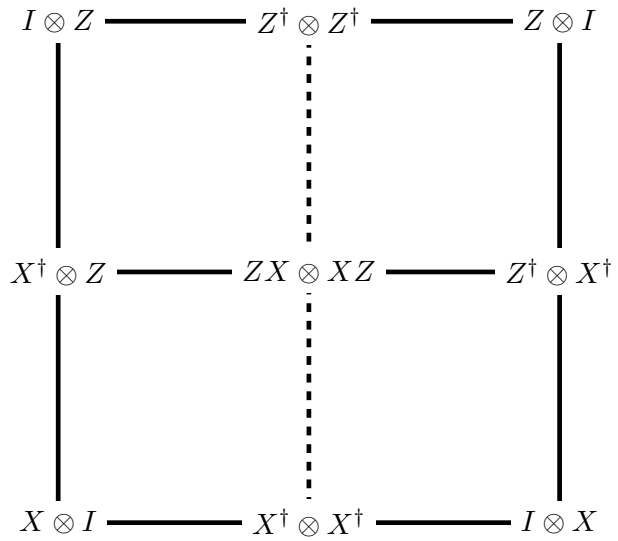
win if they return assignments that satisfy the queried equations and, moreover, their answers are consistent, meaning that they assign the same value to overlapping variables. It is not difficult to see that a classical strategy winning with perfect probability exists if and only the system of equations has a solution. In the quantum case, this is not true, and the Magic Square game described earlier is a counterexample. In Subsections 3.5.1, 3.5.2, and 3.5.3, we introduce the necessary group and representation theoretic background and notation. In Subsection 3.5.4, we give a more formal introduction to LCS games. In Subsection 3.5.5, we prove our self-testing theorem for LCS games satisfying certain properties. In Subsection 3.5.6, we apply this theorem to the Magic Square and Magic Pentagram games.

3.5.1 Groups

We work with several groups via their presentations. For the basic definitions of group, quotient group, etc. see any abstract algebra text, e.g. [32].

Definition 13. *Let S be a set of letters. We denote by $\mathcal{F}(S)$ the* free group on S. *As a set, $\mathcal{F}(S)$ consists of all finite words made from $\left\{s, s^{-1} \,\middle|\, s \in S\right\}$ such that no ss^{-1} or $s^{-1}s$ appears as a*

Figure 3.3: On the left are the operators of the Magic Square. X and Z are the Pauli operators (we use this notation here instead of σ_Z and σ_X as it is visually clearer). Across any solid line, the three operators commute and their product is identity. Across the dashed line, the operators commute and their product is -1 times identity.



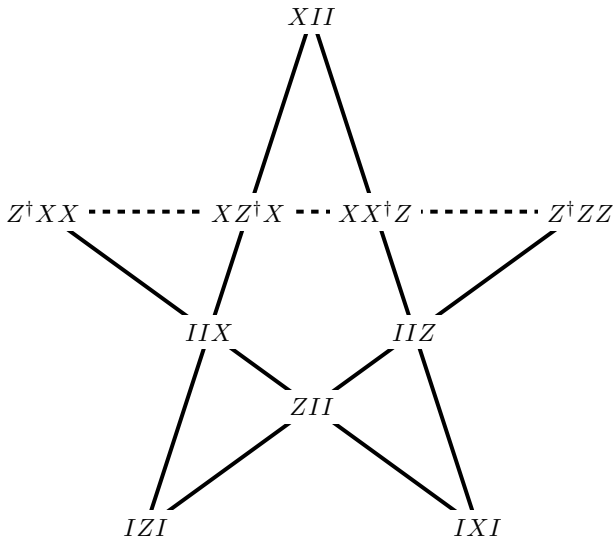


Figure 3.4: On the right are the operators of the Magic Pentagram. These are operators on $(\mathbb{C}^2)^{\otimes 3}$; the tensor product symbols are omitted. Across any line, the four operators commute. Across any solid line, the alternating product $AB^\dagger CD^\dagger$ of the four operators is identity. Across the dashed line, the alternating product (computed from left to right) is -1 times identity.

substring for any s. The group law is given by concatenation and cancellation.

Definition 14 (Group presentation)**.** *Let S be finite and R a finite subset of $\mathcal{F}(S)$. Then $G = \langle S : R \rangle$ is the* finitely presented group *generated by S with relations from R. Explicitly, $G = \mathcal{F}(S) / \langle R \rangle$, where $/$ is used to denote the quotient of groups, and $\langle R \rangle$ denotes the subgroup generated by R. We say that an equation $w = w'$ is* witnessed by *R if $w'w^{-1}$ (or some cyclic permutation thereof) is a member of R.*

We emphasize that in this work, we sometimes distinguish between two presentations of the same group. If $G = \langle S : R \rangle, G' = \langle S' : R' \rangle$ are two finitely presented groups, we reserve equality for the case $S = S'$ and $R = R'$, and in this case we'll say $G = G'$. We'll say that $G \cong G'$ if there is a group isomorphism between them.

Definition 15. *Let $G = \langle S : R \rangle$ be a finitely presented group and $\mathsf{can} : G \to \mathcal{F}(S)$ be an injective function. We say that can is a* canonical form *for G if the induced map $\bar{\mathsf{can}} : G \to \mathcal{F}(S) / \langle R \rangle$ is an isomorphism. In other words, we require that $\mathsf{can}(g)\,\mathsf{can}(h) = \mathsf{can}(gh)$ as elements of G, but not as strings.*

Now and throughout the paper, for a group G, we'll denote by 1 its identity, and we'll let $[a, b] := aba^{-1}b^{-1}$ denote the commutator of a and b. The group presentations of interest in this paper will take a special form extending the "groups presented over $\mathbb{Z}_2$" from [90].

Definition 16 (Group presentation over $\mathbb{Z}_d$)**.** *Let $d \in \mathbb{N}$ and let $\mathbb{Z}_d = \langle J : J^d \rangle$ be the finite cyclic group of order d. A* group presented over $\mathbb{Z}_d$ *is a group $G = \langle S' : R' \rangle$, where S' contains a distinguished element J and R' contains relations $[s, J]$ and s^d for all $s \in S$.*

For convenience, we introduce notation that suppresses the standard generator J and the standard relations:

$$G = \langle S : R \rangle_{\mathbb{Z}_d} = \left\langle S \cup \{J\} : R \cup \left\{ s^d, J^d, [s, J] \,\middle|\, s \in S \right\} \right\rangle .$$

In the group representations of interest, we'll have $J \mapsto e^{2\pi i/d}$—we should always just think of J as a d^{th} root of unity. We'll think of relations of the form $J^{-1}[a, b]$ as "twisted commutation" relations, since they enforce the equation $aba^{-1}b^{-1} = e^{2\pi i/d}$.

Example 1. *The Pauli group on one d-dimensional qudit can be presented as a group over $\mathbb{Z}_d$:*

$$\mathcal{P}_d^{\otimes 1} = \langle x, z : J[x, z] \rangle_{\mathbb{Z}_d} .$$

3.5.2 Group pictures

Suppose we have a finitely presented group $G = \langle S : R \rangle$ and a word $w \in \mathcal{F}(S)$ such that $w = 1$ in G. Then by definition, there is a way to prove that $w = 1$ using the relations from R. How complicated can such a proof get? Group pictures give us a way to deal with these proofs graphically, rather than by writing long strings of equations. In particular, we will use group pictures to get quantitative bounds on the length of such proofs. (For a more mathematically rigorous treatment of group pictures, see [90]. These are dual to what are usually known as van Kampen diagrams.)

Definition 17 (Group picture)**.** *Let $G = \langle S : R \rangle_{\mathbb{Z}_d}$ be a group presented over $\mathbb{Z}_d$. A G-picture is a labeled drawing of a planar directed graph in the disk. Some vertices may lie on the boundary. The vertices that do not lie on the boundary are referred to as* interior vertices*. A G-picture is* valid *if the following conditions hold:*

- *Each interior vertex is labeled with a power of J. (We omit the identity label.)*
- *Each edge is labeled with a generator from S.*
- *At each interior vertex v, the clockwise product of the edge labels (an edge labeled s should be interpreted as s if it is outgoing and as s^{-1} if it is ingoing) is equal to the vertex label, as witnessed by R. (Since the values of the labels are in the center of the group, it doesn't matter where you choose to start the word.)*

Note that the validity of a G-picture depends on the presentation of G. Pictures cannot be associated directly with abstract groups.

If we collapse the boundary of the disk to a point ("the point at infinity"), then the picture becomes an embedding of a planar graph on the sphere (see Figure 3.5). The following is a kind of "Stoke's theorem" for group pictures, which tells us that the relation encoded at the point at infinity is always valid.

Definition 18. *Suppose $\mathcal{P}$ is a G-picture. The* boundary word *w is the product of the edge labels of the edges incident on the boundary of $\mathcal{P}$, in clockwise order.*

Lemma 4 (van Kampen)**.** *Suppose $\mathcal{P}$ is a valid G-picture with boundary word w. Let J^a be the product of the labels of the vertices in $\mathcal{P}$. Then $w = J^a$ is a valid relation in G. Moreover, we say that the relation $w = J^a$ is* witnessed *by the G-picture $\mathcal{P}$.*

The proof is elementary and relies on the fact that the subgroup $\langle J | J \rangle$ is abelian and central, so that cyclic permutations of relations are valid relations.

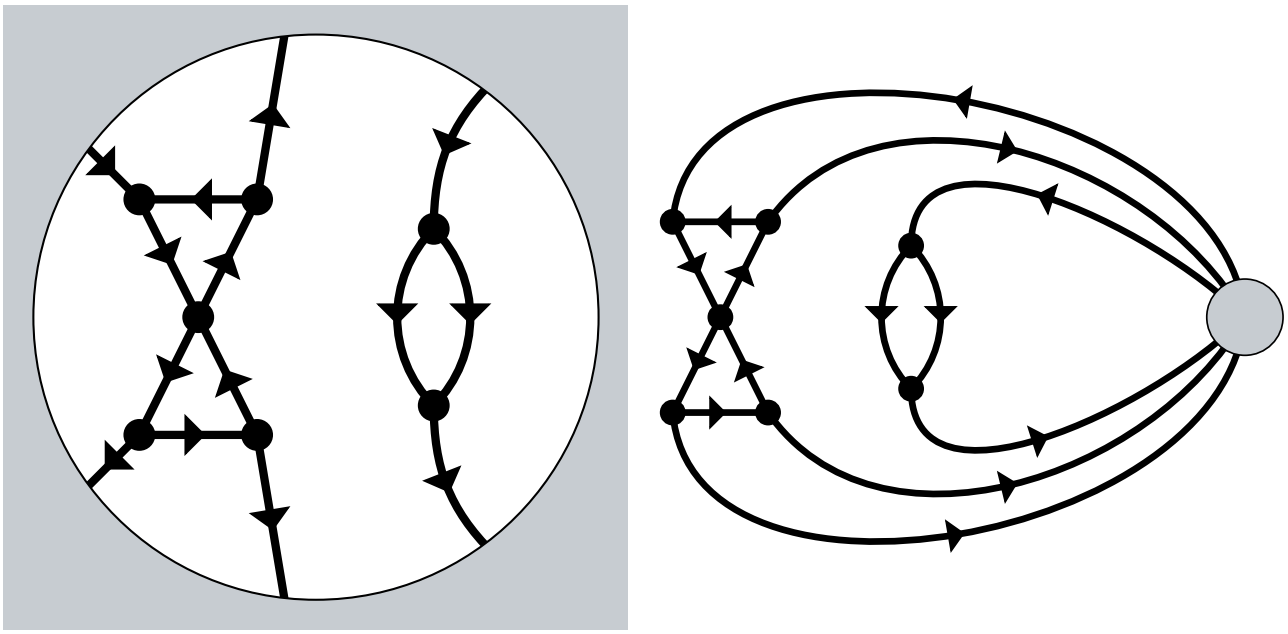
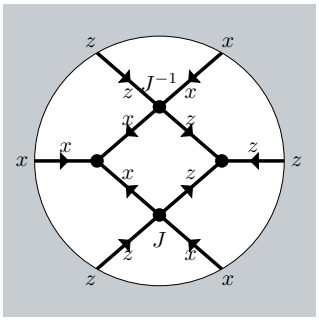
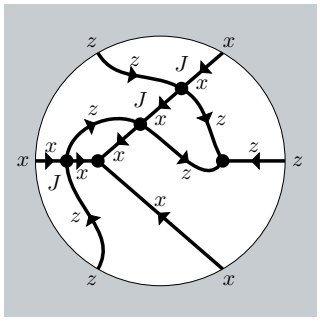


Figure 3.5: This is a directed version of Figure 3 from [90] . The interior vertices are drawn with dots, while the edge labels and the non-interior vertices are suppressed.

Example 2. *Recall the group $\mathcal{P}_d^{\otimes 1}$ from Example 1. It's easy to see that $(xz)^d = 1$ in this group. In Figure 3.6, we give two proofs of this fact, for the case $d = 3$. The examples are chosen to illustrate that shorter proofs are more natural than longer proofs in the group picture framework.*

$$
\begin{aligned}
&(zx)z(xz)x \\
&= (Jxz)z(J^{-1}zx)x \\
&= x(zzz)xx \\
&= (xxx) \\
&= 1
\end{aligned}
$$





$$
\begin{aligned}
&(zx)zxzx \\
&= Jxz(zx)zx \\
&= J^2x(zx)zzx \\
&= xx(zzz)x \\
&= (xxx) \\
&= 1
\end{aligned}
$$

Figure 3.6: The first picture uses a minimal number of relations, and corresponds (in an imprecise sense) to the equation manipulations on the left. The second picture corresponds to the equation manipulations on the right, in which each z is commuted all the way to the end of the string.

3.5.3 Representation theory of finite groups

We'll study groups through their representations. We collect here some basic facts about the representation theory of finite groups. For exposition and proofs, see e.g. [32]. Throughout, G will be a finite group. It should be noted that some of these facts are not true of infinite groups.

Definition 19. *A d-dimensional* representation *of G is a homomorphism from G to the group of invertible linear operators on $\mathbb{C}^d$. A representation is* irreducible *if it cannot be decomposed as a direct sum of two representations, each of positive dimension. A representation is* trivial *if its image is $\{I\}$, where I is the identity matrix. The* character *of a representation σ is the function defined by $g \mapsto \mathrm{Tr}(\sigma(g))$. Two representations ρ_1 and ρ_2 are* equivalent *if there is a unitary U such that for all g, $U\rho_1(g)U^\dagger = \rho_2(g)$.*

Notice that a 1-dimensional representation and its character are the same function, and that 1-dimensional representations are always irreducible. We sometimes write "irrep" for "irreducible representation." The next fact allows us to check equivalence of representations algebraically.

Fact 1. *ρ_1 is equivalent to ρ_2 iff they have the same character.*

The following is immediate:

Lemma 5. *Let $\sigma = \bigoplus_i \sigma_i$ be a direct sum decomposition of σ into irreducibles. Let $\circ$ denote composition of maps, and let $\chi = \mathrm{Tr} \circ \sigma, \chi_i = \mathrm{Tr} \circ \sigma_i$ be the characters corresponding to the representations σ. Then $\chi = \sum_i \chi_i$.*

Furthermore, define $\tilde{\chi} = \frac{1}{\dim \sigma}\chi$ and $\tilde{\chi}_i = \frac{1}{\dim \sigma_i}\chi_i$ as the normalized characters *of σ, σ_i. Then the normalized character of σ is a convex combination of the normalized characters of σ_i.*

$$\tilde{\chi} = \sum_i \frac{\dim \sigma_i}{\dim \sigma} \tilde{\chi}_i \,.$$

There is a simple criterion to check whether a representation of a finite group is irreducible:

Fact 2. *σ is an irreducible representation of G iff*

$$|G| = \sum_{g \in G} \mathrm{Tr}\, \sigma(g)\, \mathrm{Tr}\, \sigma(g^{-1}) \,.$$

Definition 20. *The* commutator subgroup *$[G, G]$ of G is the subgroup generated by all elements of the form $[a, b] := aba^{-1}b^{-1}$ for $a, b \in G$. The* index *$|G : H|$ of a subgroup $H \leq G$ is the number of H-cosets in G. Equivalently for finite groups, the index is the quotient of the orders $|G : H| = \frac{|G|}{|H|}$.*

Fact 3. *G has a number $|G : [G,G]|$ of inequivalent 1-dimensional irreducible representations, each of which restricts to the trivial representation on $[G,G]$.*

Fact 4. *For a finite group G, the size of the group is equal to the sum of the squares of the dimensions of the irreducible representations. In other words, for R any set of inequivalent irreps,*

$$|G| = \sum_{\sigma \in R} (\dim \sigma)^2 \text{ iff } R \text{ is maximal.} \tag{3.15}$$

By "maximal", we mean that any irreducible representation is equivalent to one from R. This fact can be used to check whether one has a complete classification of the irreducibles of G. This is a special case of the following for $x = 1$.

Fact 5 (Second orthogonality relation for character tables)**.** *Let $x \in G$. Let σ vary over a maximal set of inequivalent irreps of G, and let n_σ be the dimension of σ. Then*

$$\frac{1}{|G|} \sum_{\sigma} n_\sigma \operatorname{Tr}(\sigma(x)) = \delta_{x,1} .$$

Fact 6 (Schur's lemma)**.** *Let $\tau : G \to U(\mathbb{C}^d)$ be an irrep and $X \in \mathcal{L}(\mathbb{C}^d)$ be a linear operator. Suppose that $X\tau(g) = \tau(g)X$ for all $g \in G$. Then $X = \lambda I$ is a scalar multiple of identity.*

3.5.4 Linear constraint system games over $\mathbb{Z}_d$

We recall several definitions from previous works of Cleve, Liu, Mittal, and Slofstra [90, 18, 19]. Following a suggestion from [18], we define the machinery over $\mathbb{Z}_d$ instead of $\mathbb{Z}_2$.

Definition 21. *A* hypergraph $\mathbf{H} = (V, E, H)$ *consists of a finite* vertex set V*, a finite* edge set E *and an* incidence matrix $H : V \times E \to \mathbb{Z}$.

We think of V as a set of $\mathbb{Z}$-linear equations, E as a set of variables, and $H(v,e)$ as the coefficient of variable e in equation v. Following Arkhipov [6], some of our hypergraphs of interest will be graphs. Unlike previous works, we introduce signed coefficients (outgoing edges have a positive sign in the incidence matrix, while ingoing edges have a negative sign). This is because previous works considered equations over $\mathbb{Z}_2$, where $1 = -1$.

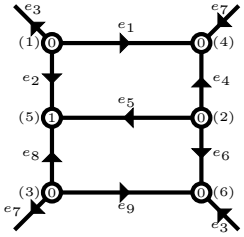
Definition 22 ([19], [90])**.** *Given hypergraph $\mathbf{H}$, vertex labelling $l : V \to \mathbb{Z}$, and some modulus $d \in \mathbb{Z}$, we can associate a nonlocal game which we'll call the* linear constraint game $\mathsf{LCS}(\mathbf{H}, l, \mathbb{Z}_d)$*. Informally, a verifier sends one equation x to Alice and one variable y to Bob, demanding an assignment $a : E \to \mathbb{Z}_d$ to all variables from Alice and an assignment $b \in \mathbb{Z}_d$ to variable y from Bob. The verifier checks that Alice's assignment satisfies equation $x \pmod d$, and that Alice and Bob gave the same assignment to variable y.*

Formally, we have the following question and answer sets: $X = V$, $Y = E$, $A = \mathbb{Z}_d^E$, $B = \mathbb{Z}_d$. *The win condition selects those tuples* (a, b, x, y) *satisfying:*

$$a(y) = b \qquad \textit{(Consistency)}$$
$$\sum_{e \in E} H(x,e)a(e) \equiv l(x) \pmod{d}. \qquad \textit{(Constraint satisfaction)}$$

We introduce the two primary LCS games of interest in this paper.

Example 3. *The magic square LCS (mod* 2*) has vertex set* $\{v_1, \ldots, v_6\}$, *edge set* $\{e_1, \ldots, e_9\}$, *vertex labeling* $l(v_5) = 1, l(v_i) = 0$ *for* $i \neq 5$. *See Figure 3.7 for the full description of the hypergraph and the associated set of linear equations.*



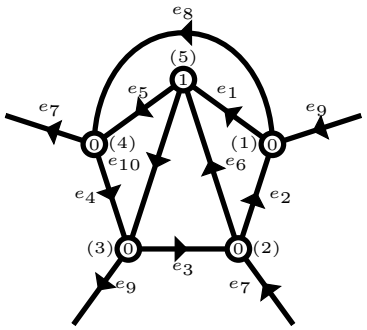
$$(1)\quad e_1 + e_2 + e_3 = 0 \qquad (4)\quad -(e_1 + e_4 + e_7) = 0$$
$$(2)\quad e_4 + e_5 + e_6 = 0 \qquad (5)\quad -(e_2 + e_5 + e_8) = 1$$
$$(3)\quad e_7 + e_8 + e_9 = 0 \qquad (6)\quad -(e_3 + e_6 + e_9) = 0$$

Figure 3.7: The magic square LCS, presented both in terms of equations (mod 2) and in terms of a labelled hypergraph. The two line segments labeled e_3 are parts of the same edge, as are the pair of line segments labeled e_7. The underlying graph is $K_{3,3}$, the smallest bipartite non-planar graph. The direction of the edges emphasizes the bipartition.

Example 4. *The magic pentagram LCS (mod* 2*) has vertex set* $\{v_1, \ldots, v_5\}$, *edge set* $\{e_1, \ldots, e_{10}\}$, *vertex labeling* $l(v_5) = 1, l(v_i) = 0$ *for* $i \neq 5$. *See Figure 3.8 for the full description of the hypergraph and the associated set of linear equations.*

The following is the main tool we use to understand linear constraint system games.

Definition 23 (Solution group over $\mathbb{Z}_d$, [18])**.** *For an LCS game* $\mathsf{LCS}(\mathbf{H}, l, \mathbb{Z}_d)$ *with* $\mathbf{H} = (V, E, H)$, *the* solution group $\Gamma(\mathbf{H}, l, \mathbb{Z}_d)$ *has one generator for each edge of* $\mathbf{H}$ *(i.e. for each variable of the linear system), one relation for each vertex of* $\mathbf{H}$ *(i.e. for each equation of the linear system), and relations enforcing that the variables in each equation commute. Formally, define the sets of relations* R_c, *the local commutativity relations, and* R_{eq}, *the constraint satisfaction relations*



$$
\begin{aligned}
&(1) && e_1 - e_2 + e_8 - e_9 = 0\\
&(2) && e_2 - e_3 + e_6 - e_7 = 0\\
&(3) && e_3 - e_4 + e_9 - e_{10} = 0\\
&(4) && e_4 - e_5 + e_7 - e_8 = 0\\
&(5) && e_5 - e_6 + e_{10} - e_1 = 1
\end{aligned}
$$

Figure 3.8: The magic pentagram LCS, presented both in terms of equations (mod 2) and in terms of a labelled hypergraph. The two line segments labeled e_7 are parts of the same edge, as are the pair of line segments labeled e_9. The underlying graph is K_5, the smallest complete non-planar graph.

as

$$
\begin{aligned}
R_c &:= \left\{ [e, e'] \,\middle|\, H(v,e) \neq 0 \neq H(v,e') \text{ for some } v \in V \right\}\\
R_{eq} &:= \left\{ J^{-l(v)} \prod_{e \in E} e^{H(v,e)} \,\middle|\, v \in V \right\}.
\end{aligned}
$$

Then define the solution group as

$$
\Gamma(\mathbf{H}, l, \mathbb{Z}_d) := \left\langle E : R_c \cup R_{eq} \right\rangle_{\mathbb{Z}_d}.
$$

(Notice that the order of the products defining R_{eq} is irrelevant, since each pair of variables appearing in the same R_{eq} relation also have a commutation relation in R_c.)

When the LCS game is clear from context, we'll just write Γ to denote its solution group.

Our aim is to prove that for some specific linear constraint system games, strategies that win with high probability are very close to some ideal form. We start by observing that for any LCS game, *any* strategy already has a slightly special form.

Lemma 6 (Strategies presented via observables)**.** *Suppose that $p(a,b\|v,e) = \mathrm{Tr}_\rho \, \tilde{A}_v^a \otimes \tilde{B}_e^b$ is a quantum strategy for an LCS game over $\mathbb{Z}_d$ with hypergraph $\mathbf{H} = (H, V, E)$. Then there are unitaries $\left\{ A_e^{(v)} \,\middle|\, e \in E, v \in V \right\}$ and $\{B_e \,|\, e \in E\}$ such that for all v, e, $(A_e^{(v)})^d = I = B_e^d$; for any fixed v, the $A_e^{(v)}$ pairwise commute; moreover, the provers win with probability 1 iff*

$$
\text{for all } v, e, \ \mathrm{Tr}_\rho \, A_e^{(v)} \otimes B_e = 1, \text{ and} \tag{3.16}
$$

$$
\text{for all } v, \ \mathrm{Tr}_\rho \prod_e \left(A_e^{(v)} \right)^{H(v,e)} \otimes I_B = \omega_d^{l(v)}. \tag{3.17}
$$

We refer to the operators $\left\{A_e^{(v)}\right\}, \{B_e\}$ together with the state ρ as a *strategy presented via observables*. Typically the word "observable" is reserved for Hermitian operators. Nonetheless, we call our operators observables because they capture properties of the projective measurements from which they're built in a useful way. Operationally, we think of Bob as measuring the observable B_e and reporting the outcome when asked about variable e and of Alice measuring the observables $A_e^{(v)}$ and reporting the outcome for each e when asked about equation v. The fact that Alice's observables pairwise commute at each equation means that Alice can measure them simultaneously without ambiguity.

A version of this lemma is proved in the course of the proof of Theorem 1 of [19]. We give essentially the same proof, just over $\mathbb{Z}_d$.

Proof of Lemma 6. Define the observables as

$$B_e := \sum_j \omega_d^{-j} \tilde{B}_e^i \qquad\qquad A_e^{(v)} := \sum_i \omega_d^i \sum_{a:a(e)=i} \tilde{A}_v^a.$$

It's clear that each of these operators is a unitary whose eigenvalues are d^{th} roots of unity. To see that $A_e^{(v)}$ commutes with $A_{e'}^{(v)}$, notice that they are different linear combinations of the same set of projectors. Now we compute, for any v, e,

$$\begin{aligned}\operatorname{Tr}_\rho A_e^{(v)} \otimes B_e &= \sum_{i,j} \omega_d^{i-j} \operatorname{Tr}_\rho \left(\sum_{a:a(e)=i} \tilde{A}_v^a \right) \otimes \tilde{B}_e^j \\ &= \sum_k \omega_d^k \Pr[a(e) - b \equiv k \mid \text{questions } x = v, y = e].\end{aligned}$$

Notice that the last line is a convex combination of the d^{th} roots of unity. Hence, it equals 1 if and only if $\Pr[a(e) \equiv b \mid \text{questions } x = v, y = e] = 1$.

A similar computation reveals:

$$\begin{aligned}&\omega_d^{-l(v)} \operatorname{Tr}_\rho \prod_e \left(A_e^{(v)}\right)^{H(v,e)} \otimes I \\ &= \sum_k \omega_d^{k-l(v)} \operatorname{Tr}_\rho \sum_{\substack{a: \\ \sum_e H(v,e)a(e) \equiv k}} \tilde{A}_v^a \otimes I \\ &= \sum_k \omega_d^{k-l(v)} \Pr\left[\sum_e H(v,e)a(e) \equiv k \middle| \text{question } x = v \right].\end{aligned}$$

Again, the last line is a convex combination of the d^{th} roots of unity. Hence it equals 1 if and only if $\Pr\left[\sum_e H(v,e)a(e) \equiv l(v) | \text{question } x = v\right] = 1$. □

Note that we can always recover the original strategy in terms of projective measurements by looking at the eigenspaces of the observables. Therefore, we restrict our attention to strategies presented by observables without loss of generality.

Next, we state a simple sufficient condition for the existence of a perfect quantum strategy for an LCS game.

Definition 24 (Operator solution)**.** *An* operator solution *for the game* $\mathsf{LCS}(\mathbf{H}, l, \mathbb{Z}_d)$ *is a unitary representation* σ *of the group* $\Gamma(\mathbf{H}, l, \mathbb{Z}_d)$ *such that* $\sigma(J) = \omega_d I$*. A* conjugate operator solution *is a unitary representation sending* $J \mapsto \overline{\omega_d} I$*.*

Notice that if σ is an operator solution, then for any choice of basis the complex conjugate $\bar{\sigma} : g \mapsto \overline{\sigma(g)}$ is a conjugate operator solution. The existence of an operator solution is sufficient to construct a perfect quantum strategy.

Example 5 (Operator solution for magic square)**.** *See the square of group generators in Figure 3.9. Let* Γ_2 *be the solution group of the Magic Square. Consider the map* $\Gamma_2 \to U(\mathbb{C}^2 \otimes \mathbb{C}^2)$ *generated by sending each generator in this square to the operator in the corresponding location of Figure 3.3. This map is an operator solution.*

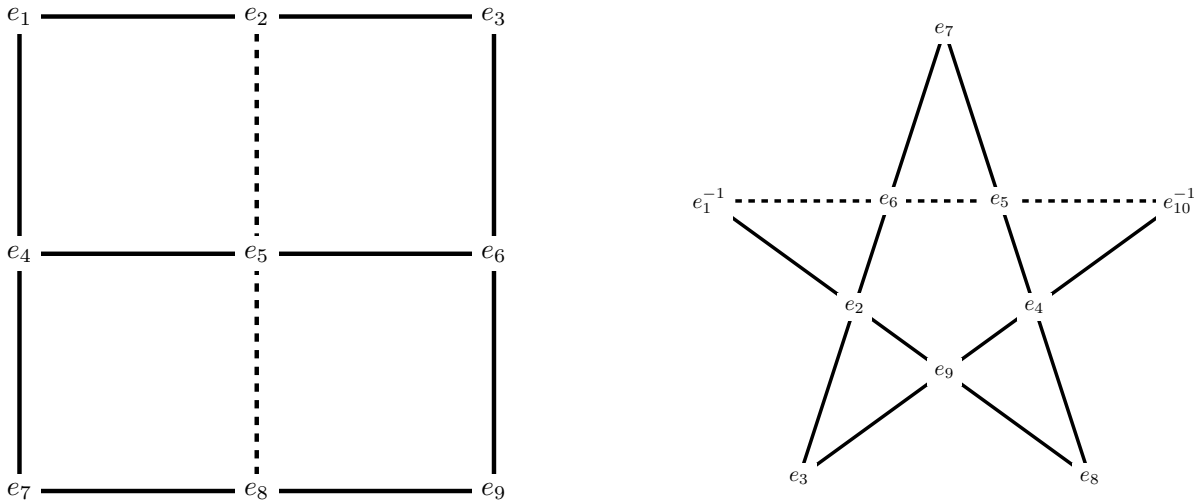


Figure 3.9: On the left-hand figure, the product of the generators on any solid line is equal to 1 in the solution group of the magic square. The product of the operators on the dashed line is equal to J. Similarly, on the right-hand figure, the alternating product $ab^{-1}cd^{-1}$ is equal to 1 on the solid lines and J on the dashed line.

Example 6 (Operator solution for magic pentagram)**.** *See the pentagram of group generators in Figure 3.9. Let* Γ_3 *be the solution group of the Magic Pentagram. Consider the map* $\Gamma_3 \to$

$U(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2)$ *generated by sending each generator in this pentagram to the operator in the corresponding location of Figure 3.3. This map is an operator solution.*

Proposition 1. *Let $\sigma : \Gamma \to U(\mathbb{C}^D)$ be an operator solution. Define a strategy by setting $|\psi\rangle = |EPR_D\rangle$, $A_e^{(v)} = \sigma(e)$ for all e, v, and $B_e = \overline{\sigma(e)}$ for all e. Provers using this strategy win with probability* 1.

Proof. By a well-known property of the maximally entangled state, we have

$$\langle\psi| \sigma(e) \otimes \overline{\sigma(e)} |\psi\rangle = \langle\psi| \sigma(e)\overline{\sigma(e)}^T \otimes I |\psi\rangle = 1,$$

where ^{T} denotes the transpose. Therefore, the consistency criterion (3.16) is satisfied. Since σ is an operator solution, we have

$$\begin{aligned}\prod_e \left(A_e^{(v)}\right)^{H(v,e)} &= \sigma(\prod_e \sigma(e)^{H(v,e)}) \\ &= \sigma(J^{l(v)}) \\ &= \omega_d^{l(v)} I,\end{aligned}$$

so the constraint satisfaction criterion (3.17) is satisfied. □

We will see an exact converse to this proposition in the next section.

3.5.5 Exact self-testing

In this section, we build up to our self-testing theorem for LCS games (in its exact form), Theorem 4. We refer the reader to [24] for the approximate version. The statement of the theorem is the following:

Theorem 4. *Let G be an LCS game over $\mathbb{Z}_d$ with vertex set V, edge set E, and constraints given by $H : V \times E \to \mathbb{Z}_d$ and $l : V \to \mathbb{Z}_d$. Let Γ be the solution group of G. Suppose that Γ is finite and all of its irreducible representations with $J \mapsto \omega_d I$ are equivalent to a fixed irrep $\sigma : \Gamma \to U(\mathbb{C}^d)$. Then G self-tests the strategy $\tilde{A}_e^{(v)} = \sigma(e), \tilde{B}_e = \overline{\sigma(e)}, |\psi\rangle = |\mathrm{EPR}_{d^n}\rangle$.*

Throughout, let $\mathsf{LCS}(\mathbf{H}, l, \mathbb{Z}_d), \mathbf{H} = (V, E, H)$ be an LCS game with solution group Γ. We start with a theorem that characterizes the observables. We will then characterize the state in Subsection 3.5.5

Theorem 5 (Characterizing the observables)**.** *Suppose Γ is finite and all of its irreducible representations with $J \mapsto \omega_d I$ are equivalent to a fixed irrep $\sigma : \Gamma \to U(\mathbb{C}^d)$. Suppose $\left\{A_e^{(v)}\right\}, \{B_e\}, \rho \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a perfect strategy presented via observables for the game. Then there are local isometries V_A, V_B such that*

- *for all e, v, $V_A A_e^{(v)} V_A^\dagger = \sigma(e) \otimes I \oplus \hat{A}_e^{(v)}$, where $\hat{A}_e^{(v)} V_A \rho V_A^\dagger = 0$, and*
- *for all e $V_B B_e V_B^\dagger = \overline{\sigma(e)} \otimes I \oplus \hat{B}_e$, where $\hat{B}_e V_B \rho V_B^\dagger = 0$.*

Formally, we must pick a basis to take the complex conjugate in. Fortunately, we only care about our operators up to isometry. So to make sense of the theorem statement, we pick the basis for complex conjugation first, and then the isometry V_B depends on this choice.

We break the proof into two lemmas.

Lemma 7. *Suppose Γ is finite and all of its irreducible representations with $J \mapsto \omega_d I$ are equivalent to a fixed irrep $\sigma : \Gamma \to U(\mathbb{C}^d)$. Then every operator solution is equivalent to $\sigma \otimes I$ and every conjugate operator solution is equivalent to $\bar{\sigma} \otimes I$, where the complex conjugate can be taken in any basis.*

Lemma 8 (Adapted from Lemma 8, [18])**.** *Suppose $\left\{A_e^{(v)}\right\}, \{B_e\}, \rho \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a perfect strategy presented via observables for the game. Then, there are orthogonal projections P_A, P_B such that*

1. *$(P_A \otimes P_B)\rho(P_A \otimes P_B) = \rho$;*
2. *for each e, $P_A A_e^{(v)} P_A = P_A A_e^{(v')} P_A$, provided that $H(v,e) \neq 0 \neq H(v',e)$ (we now write $P_A A_e P_A$ without ambiguity);*
3. *the map $\sigma_A : \Gamma \to \operatorname{ran} P_A$ generated by $e \mapsto P_A A_e P_A$ (and $j \mapsto \omega_d I$) is an operator solution;*
4. *the map $\sigma_B : \Gamma \to \operatorname{ran} P_B$ generated by $e \mapsto P_B B_e P_B$ (and $j \mapsto \overline{\omega_d} I$) is a conjugate operator solution.*

Proof of Theorem 5, assuming the lemmas. Take the maps σ_A and σ_B from Lemma 8; note that their ranges are the subspaces determined by P_A, P_B. From Lemma 7 we get partial isometries W_A, W_B such that $W_A \sigma_A(e) W_A^\dagger = \sigma(e) \otimes I$ and $W_B \sigma_B(e) W_B^\dagger = \overline{\sigma(e)} \otimes I$. To complete the proof, let V_A and V_B be any isometric extensions of W_A and W_B, and set $\hat{A}_e^{(v)} = V_A(I - P_A)A_e^{(v)}(I - P_A)V_A^\dagger, \hat{B}_e = V_B(I - P_B)B_e(I - P_B)V_B^\dagger$. Checking that these operators satisfy the equations in the theorem is a simple computation. □

Proof of Lemma 7. Let τ be an operator solution, i.e. a representation of Γ with $\tau(J) = \omega_d I$. Let $\tau = \oplus_{i=1}^k \tau_i$ be a decomposition of τ into k irreducibles. As in Lemma 5, let $\tilde{\chi} : g \mapsto \frac{1}{\dim \tau} \operatorname{Tr} \tau(g)$ be the normalized character of τ and $\tilde{\chi}_i$ be the same for τ_i. One can check that $|\tilde{\chi}_i(g)| \leq 1$ for all

$g \in \Gamma$. Furthermore, $\tilde{\chi}(g)$ is a convex combination of the $\chi_i(g)$. Therefore, $\tilde{\chi}_i(J) = \omega_d$ for each i. Then also $\tau_i(J) = \omega_d I$ for each i, since this the only d-dimensional unitary with trace $d\omega_d$. We conclude that τ is equivalent to $\bigoplus_{i=1}^{k} \sigma = \sigma \otimes I_k$.

Now suppose that τ' is a conjugate operator solution. Then taking the complex conjugate in any basis, $\overline{\tau'}$ is an operator solution. By the above, $\overline{\tau'}$ is equivalent to $\sigma \otimes I$. Therefore, τ' is equivalent to $\bar{\sigma} \otimes I$. □

Proof of Lemma 8. This is essentially the same proof as given in [18] (their treatment is a bit more complicated since they wish to cover the infinite-dimensional case).

Let $\mathcal{A}$ be the set of finite products of unitaries from $\left\{ A_e^{(v)} \right\}$, and similarly let $\mathcal{B}$ be the set of finite products of unitaries from $\{B_e\}$. Let $\rho_A = \mathrm{Tr}_B \rho$ and $\rho_B = \mathrm{Tr}_A \rho$. Define

$$\hat{\mathcal{H}_A} = \mathrm{supp}\, \rho_A \,, \text{and } \hat{\mathcal{H}_B} = \mathrm{supp}\, \rho_B \,,$$

and let P_A and P_B be the projectors onto these spaces. Notice that $(P_A \otimes P_B)\rho(P_A \otimes P_B) = \rho$. From the consistency criterion (3.16), we have

$$1 = \mathrm{Tr}_\rho\, A_e^{(v)} \otimes B_e, \text{ so } A_e^{(v)} \left|\phi\right\rangle = B_e^\dagger \left|\phi\right\rangle \text{ for } \left|\phi\right\rangle \in \mathrm{supp}\, \rho \,. \tag{3.18}$$

Let $A \in \mathcal{A}$ be arbitrary. Then, the above implies that there is $B \in \mathcal{B}$ be such that $(A \otimes I)\rho(A^\dagger \otimes I) = (I \otimes B^\dagger)\rho(I \otimes B)$. We compute

$$A\rho_A A^\dagger = \mathrm{Tr}_B (A \otimes I)\rho(A^\dagger \otimes I) = \mathrm{Tr}_B (I \otimes B^\dagger)\rho(I \otimes B) = \mathrm{Tr}_B\, \rho = \rho_A \,,$$

from which we conclude that $\mathcal{A}$ fixes $\hat{\mathcal{H}_A}$. This implies that $(PA_1P)(PA_2P) = PA_1A_2P$ for $A_1, A_2 \in \mathcal{A}$. Next, we compute

$$1 = \mathrm{Tr}_\rho\, A_e^{(v)} (A_e^{(v')})^\dagger \otimes I = \mathrm{Tr}_{\rho_A}\, A_e^{(v)} (A_e^{(v')})^\dagger \,,$$

from which we conclude that $P_A A_e^{(v)} P_A = P_A A_e^{(v')} P_A$. We now write $P_A A_e P_A$ without ambiguity. Finally, we compute

$$1 = \mathrm{Tr}_\rho\, w_d^{-l(v)} \prod_{e:H(v,e)\neq 0} A_e \otimes I = \mathrm{Tr}_{\rho_A}\, w_p^{-l(v)} \prod_{e:H(v,e)\neq 0} A_e \otimes I \,,$$

from which we conclude that the map $e \mapsto P_A A_e P_A$ is an operator solution. The same argument shows that $e \mapsto P_B B_e P_B$ is a conjugate operator solution. (The conjugation comes from equation (3.18).) □

Stabilizer state bounds We show that if a state is stabilized by the simultaneous action of an irreducible group representation on two tensor factors, then the state is maximally entangled between those factors. This will allow us to deduce self-testing of the provers' state from the characterization of their observables from Theorem 5.

Lemma 9. *Let $\tau : \Gamma \to U(\mathbb{C}^d)$ be an irreducible representation with Γ a finite group. Then the maximally entangled state can be characterized as a uniform combination of operators from the image of $\tau \otimes \overline{\tau}$. In particular,*

$$|EPR_d\rangle\langle EPR_d| = \mathop{\mathbb{E}}_{g\in\Gamma} \tau(g) \otimes \overline{\tau(g)}\,.$$

Proof. We show four intermediate equations via simple computations.

1. $\rho_{AB} = \rho_{AB}^\dagger$
2. $\operatorname{Tr} \rho_{AB} = 1$
3. $\rho_{AB}^2 = \rho_{AB}$
4. $\operatorname{Tr}_B \rho_{AB}$ is maximally mixed.

The first two items assert that ρ_{AB} is a density matrix. The third shows that it is in fact pure. The fourth tells us that the state is maximally entangled across the A/B cut. This characterizes the state.

Our main trick for the whole proof will be to relabel the index of summation defining ρ_{AB}. To prove the first item, we use the relabeling $x \mapsto x^{-1}$.

$$\begin{aligned}
\rho_{AB} &= \mathop{\mathbb{E}}_x \tau(x)_A \otimes \overline{\tau(x)}_B \\
&= \mathop{\mathbb{E}}_x \tau(x^{-1})_A \otimes \overline{\tau(x^{-1})}_B \\
&= \mathop{\mathbb{E}}_x \tau(x)_A^\dagger \otimes \overline{\tau(x)}_B^\dagger \\
&= \left[\mathop{\mathbb{E}}_x \tau(x)_A \otimes \overline{\tau(x)}_B\right]^\dagger \\
&= \rho_{AB}^\dagger\,.
\end{aligned}$$

(Notice we've used the fact that $\tau(x)$ is unitary; this is one of several parts of the proof that relies on the finiteness of Γ.) Now define the character $\chi(x) := \operatorname{Tr} \tau(x)$ to compute:

$$\begin{aligned}
\operatorname{Tr} \rho_{AB} &= \operatorname{Tr} \mathop{\mathbb{E}}_x \tau(x)_A \otimes \overline{\tau(x)}_B \\
&= \mathop{\mathbb{E}}_x \chi(x)\overline{\chi(x)} \\
&= 1\,.
\end{aligned}$$

The final equation is true for the character of any irreducible representation character, and is referred to as the “second orthogonality relation" in Dummit and Foote [32]. For the second item,

$$\begin{aligned}
\rho_{AB}^2 &= \left(\mathop{\mathbb{E}}_x \tau(x)_A \otimes \overline{\tau(x)}_B\right)^2 \\
&= \mathop{\mathbb{E}}_x \mathop{\mathbb{E}}_y \tau(x)_A \tau(y)_A \otimes \overline{\tau(x)}_B \overline{\tau(y)}_B \\
&= \mathop{\mathbb{E}}_x \left[\mathop{\mathbb{E}}_y \tau(xy)_A \otimes \overline{\tau(xy)}_B\right] \\
&= \mathop{\mathbb{E}}_x \left[\mathop{\mathbb{E}}_y \tau(y)_A \otimes \overline{\tau(y)}_B\right] .
\end{aligned}$$

In the last line, we used the relabeling $y \mapsto xy$. Continuing, we have

$$\begin{aligned}
&= \mathop{\mathbb{E}}_x \rho_{AB} \\
&= \rho_{AB} .
\end{aligned}$$

Now define $\rho_A = \mathrm{Tr}_B \rho_{AB}$. Let $y \in \Gamma$ be arbitrary and use the relabeling $x \mapsto yxy^{-1}$:

$$\begin{aligned}
\rho_A &= \mathop{\mathbb{E}}_x \overline{\chi(x)} \tau(x) \\
&= \mathop{\mathbb{E}}_x \overline{\chi(yxy^{-1})} \tau(yxy^{-1}) \\
&= \mathop{\mathbb{E}}_x \overline{\chi(x)} \tau(y)\tau(x)\tau(y)^{-1} \\
&= \tau(y) \left[\mathop{\mathbb{E}}_x \overline{\chi(x)} \tau(x)\right] \tau(y)^{-1} \\
&= \tau(y) \rho_A \tau(y)^{-1} .
\end{aligned}$$

So ρ_A commutes with $\tau(y)$ for all y. By Schur’s lemma (Fact 6), ρ_A is a scalar multiple of identity. Since $\mathrm{Tr}\, \rho_A = 1$, we know that ρ_A is in fact the maximally mixed state.

Since the maximally entangled state of local dimension d on systems A and B is the unique pure state such that the partial trace over either system gives a maximally mixed state, this concludes our proof. □

Corollary 1. *Let $\mathcal{H}_A \cong \mathcal{H}_B \cong \mathbb{C}^d$. Let ρ_{ABC} be a state on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. Let $\rho_{AB} = \mathrm{Tr}_C \rho_{ABC}$. Let Γ be a finite group. Suppose that for each $g \in \Gamma$, $\tau(g) \otimes \overline{\tau(g)} \rho_{AB} (\tau(g) \otimes \overline{\tau(g)})^\dagger = \rho_{AB}$. Then there is a state ρ_{aux} such that $\rho_{ABC} = |EPR_d\rangle\langle EPR_d| \otimes \rho_{aux}$.*

Proof. This follows from an application of Lemma 9 and the monogamy of entanglement. □

Proof of Theorem 4. We have all the ingredients we need. The theorem follows straightforwardly from putting together Theorem 5, Corollary 1, and the consistency condition of the LCS game G. □

3.5.6 Self-testing of specific games

We now put our general self-testing theorem to use. We apply it to the Magic Square and Magic Pentagram games. We must both understand the representation theory of their abstract solution groups and the combinatorics of the presentations for those groups.

Even though our general self-testing theorem holds for LCS games mod d, we are currently only aware of applications of it to examples of LCS games mod 2. In the next subsection, we study the representation theory of the n-qudit Pauli group for a general d, even though we will only make use of it for the case of $d = 2$ and $n = 2, 3$.

3.5.6.1 The qudit pauli group

Definition 25. *The n-qudit Pauli group of local dimension d is denoted $\mathcal{P}_d^{\otimes n} := \langle S : R \rangle_{\mathbb{Z}_d}$ and presented with generators and relations*

$$S = \{x_i, z_i \,|\, i \leq n\} \qquad R = \left\{ J^{-1}[x_i, z_i], [x_i, x_j], [z_i, z_j], [x_i, z_j] \,\middle|\, i \neq j \leq n \right\}$$

We aim to show that the Pauli group is suitable for applying the results from Section 3.5.5.

Definition 26. *We now define maps $\tau_l^{(n)} : \mathcal{P}_d^{\otimes n} \to U(\mathbb{C}^d)^{\otimes n}$ as*

$$\begin{aligned}
\tau_l^{(n)}(J) &= \omega_d^l I, \\
\tau_l^{(n)}(x_i) &= \underbrace{I \otimes \cdots I}_{i-1} \otimes X^l \otimes \underbrace{I \otimes \cdots \otimes I}_{n-i}, \\
\tau_l^{(n)}(z_i) &= \underbrace{I \otimes \cdots I}_{i-1} \otimes Z \otimes \underbrace{I \otimes \cdots \otimes I}_{n-i}.
\end{aligned}$$

where X is the generalized Pauli X operator, i.e. the unitary operator on $\mathbb{C}^d$ which maps $|i\rangle \mapsto |i+1 \bmod d\rangle$, and Z is the generalized Pauli Z operator, i.e. the unitary operator on $\mathbb{C}^d$ which maps $|i\rangle \mapsto \omega_d^i |i\rangle$.

Lemma 10. *The $\left\{ \tau_l^{(n)} \,\middle|\, l \in \mathbb{Z}_d \setminus \{0\} \right\}$ are $d-1$ inequivalent representations of dimension d^n.*

Proof. To see that they are representations, it suffices to check the commutation and anticommutation relations. To see that they are inequivalent, see that their characters differ at J, since $\operatorname{Tr} \tau_l^{(n)}(J) = \omega_d^l d^n$. □

Proposition 2. *$\mathcal{P}_d^{\otimes n}$ has exactly $d-1$ irreducible representations of dimension d^n, each sending J to a different nontrivial d^{th} root of unity. All other irreducible representations are 1-dimensional and send J to 1.*

To prove this, we first establish the following lemma, which will let us count the elements of $\mathcal{P}_d^{\otimes n}$.

Lemma 11. *There is a canonical form* $\mathsf{can} : \mathcal{P}_d^{\otimes n} \to \mathcal{F}(S)$ *which sends each element to a string of the form*

$$J^{a_1} \prod_{i=1}^{n} x_i^{a_{2i}} z_i^{a_{2i+1}}, a_i \in \mathbb{Z}_d \,.$$

Proof. First, we see that each element can be written this way. Start with an arbitrary word representing the element and apply the commutation and anticommutation relations to get the x_i and z_i in order. Finish by commuting all of the Js to the front and applying the relations $s^d = 1$ to get all of the exponents to lie in $\mathbb{Z}_d$.

Next, we see that different words represent different group elements. Suppose that

$$J^{a_1} \prod_{i=1}^{n} x_i^{a_{2i}} z_i^{a_{2i+1}} = J^{b_1} \prod_{i=1}^{n} x_i^{b_{2i}} z_i^{b_{2i+1}} \,.$$

Then by various applications of the (twisted) commutation relations, we have

$$J^{c_1} = \prod_{i=1}^{n} x_i^{a_{2i}-b_{2i}} z_i^{a_{2i+1}-b_{2i+1}} \tag{3.19}$$

for some $c_1 \in \mathbb{Z}_d$. The left hand side is always central, but the right hand side is central only if $a_i = b_i$ for all $i \in [2, 2n+1]$. (Suppose for example that $a_3 - b_3 \neq 0$, so that the power of z_1 is nonzero. Then the right hand side fails to commute with x_1.) In this case, we can see that in fact $c_1 = a_1 - b_1$, so equation (3.19) holds only if $J^{c_1} = 1$ in the group. But Proposition 10 gives us a representation in which J and 1 are represented by distinct matrices. Therefore, equation (3.19) holds only when $a_i = b_i$ for all i. □

Thanks to the canonical form, we can easily compute the size of $\mathcal{P}_d^{\otimes n}$.

Corollary 2. $\mathcal{P}_d^{\otimes n}$ *has* d^{2n+1} *elements.*

Proof of Proposition 2. We will complete the character table of $\mathcal{P}_d^{\otimes n}$. Now that we know the size of the group, we can check via Fact 2 that the representations of Lemma 10 are irreducible.

Next, we notice that the commutator subgroup $[\mathcal{P}_d^{\otimes n}, \mathcal{P}_d^{\otimes n}]$ is equal to $\langle J|J\rangle$, the cyclic subgroup generated by J. This has order d, so by Fact 3, there are d^{2n} irreps of dimension 1 which send J to 1. Now we add the squares of the dimensions of our irreps and see that they saturate equation (3.15).

$$\left|\mathcal{P}_d^{\otimes n}\right| = d^{2n+1} = (d-1)\cdot(d^n)^2 + (d^{2n})\cdot(1)^2 = \sum_{\sigma} (\dim \sigma)^2 \,.$$

Therefore, we have found all irreducible representations of $\mathcal{P}_d^{\otimes n}$. □

3.5.6.2 Self-testing the Magic Square

Recall the definition of the Magic Square game from Example 3.

Definition 27 (Ideal strategy for the Magic Square LCS game $\pmod 2$)**.** *See Figure 3.10. Let A_e be the operator which appears on the right-hand side in the same spot as variable e appears on the left-hand side. Set $A_e^{(v)} := A_e$ for all v. Then set $B_e = \overline{A_e}$ (where any choice of basis works for the conjugation). Set $|\psi\rangle = |EPR\rangle^{\otimes 2}$. We define $\{A_e^{(v)}\}, \{B_e\}, |\psi\rangle$ to be the* ideal strategy *for the Magic Square game* $\pmod 2$.

Notice that the B_e are defined only up to local isometry, because of the freedom in the choice of basis for conjugation.

The robust self-testing theorem for the Magic Square game is the following.

Theorem 6. *The Magic Square game mod* 2 *self-tests the ideal strategy with perfect completeness and $O(\sqrt{\varepsilon})$-robustness.*

We will only prove the exact version. The robust version can be found in [24]. We will make a direct application of Theorem 4. Throughout, let Γ_2 be the solution group for the Magic Square game over $\mathbb{Z}_2$. The crux of the proof is identifying Γ_2 as a group of Pauli operators. We will prove the following:

Proposition 3. $\Gamma_2 \cong \mathcal{P}_2^{\otimes 2}$.

Proof of Theorem 6, assuming Proposition 3. We can apply Proposition 2 to deduce that Γ_2 has a (up to equivalence) a single irreducible representation that maps J to -1, and this is of dimension

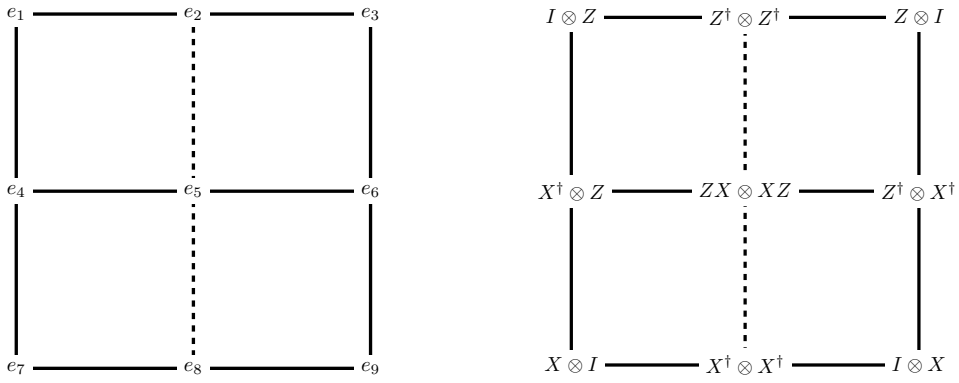


Figure 3.10: The standard operator solution for the Magic Square.

$2^2 = 4$. The operators from Figure 3.10 constitute a representation of Γ_2. This implies Theorem 6. □

We now prove Proposition 3 with two lemmas.

Lemma 12. *The commutator subgroup* $[\Gamma_2, \Gamma_2]$ *is* $\langle J \rangle$*, the cyclic subgroup generated by* J*.*

Proof. First, note that J commutes with everything by construction. Next, see that each pair of generators of Γ_2 has a commutator which is a power of J, and that J commutes with all generators. If w_1, w_2 are words in the generators, then it holds by induction on the lengths of the words that $w_1 w_2 = J^a w_2 w_1$ for some $a \in \mathbb{Z}_2$. This proves the inclusion $\Gamma_2' \subseteq \langle J \rangle$. The reverse inclusion is immediate. □

Lemma 13. *For generators* $s_1, s_2 \in \Gamma_2$*, say that the pair* $\{s_1, s_2\}$ *is* intersecting *if the corresponding edges in the constraint graph are incident on a common vertex. Let* x_1, x_2, z_1, z_2 *be any generators of* Γ_2 *such that* $\{x_1, x_2\}, \{z_1, z_2\}, \{x_1, z_2\}, \{z_1, x_2\}$ *are interesecting pairs, while* $\{x_1, z_1\}, \{x_2, z_2\}$ *are not. Then*

1. $[x_1, z_1] = J = [x_2, z_2]$*, and*
2. $\{x_1, x_2, z_1, z_2, J\}$ *generates* Γ_2*.*

Proof. 1. If x_1 and z_1 are any pair of edges not sharing a vertex, then the group picture of Figure 3.11 establishes the twisted commutation relation. If x_2 and z_2 are any other pair of edges which do not share a vertex, then there is an automorphism of the graph $K_{3,3}$ sending $x_1 \mapsto x_2$ and $z_1 \mapsto z_2$. Therefore, we can draw the same group picture with a different labeling to prove that x_2 and z_2 share the same twisted commutation relation.

2. See Figure 3.11. Suppose some vertex has only one black edge. Then the group element labeling the black edge is equal to some product of J and the group elements labeling the blue edges at that vertex. So the group generated by the blue edges and J contains the black edge. By the sequence of pictures in Figure 3.11, we see that the four blue edges, together with J, generate all nine of the edges. Therefore, they generate all of Γ_2. □

From here on, we fix the identification $x_1 = e_7, x_2 = e_9, z_1 = e_3, z_2 = e_1$ (c.f. Figure 3.10).

Proof of Proposition 3. We have the same set of generators for both groups. This gives a surjective function $\mathcal{P}_2^{\otimes 2} \to \Gamma_2$. We've seen that the generators of Γ_2 satisfy the relations defining $\mathcal{P}_2^{\otimes 2}$; this implies that the function is a group homomorphism. All that remains to check is that the map is

injective, i.e. has trivial kernel. This holds if the relations of Γ_2 hold for the preimages of the e_i in $\mathcal{P}_2^{\otimes 2}$. This follows from the fact that the square of operators (3.10) is a Mermin–Peres magic square in the usual sense, i.e. operators in the same row or column commute, the products across each row and down the first two columns are I, and the product down the last column is $-I$. *Notice that this step fails for the Magic Square game mod $d \neq 2$.*

□

3.5.6.3 Self-testing the Magic Pentagram

Recall the definition of the Magic Pentagram game from Example 4.

Definition 28 (Ideal strategy for Magic pentagram $\pmod 2$)**.** *In Figure 3.12, associate each operator in the left-hand pentagram with the corresponding variable in the right-hand pentagram. Set $A_e^{(v)}$ to the operator corresponding to e, and denote the latter by A_e, so that we have $A_e^{(v)} = A_e$ for all v. Then set $B_e = \overline{A_e}$ (where any choice of basis works for the conjugation).*

Set $|\psi\rangle = |EPR_2\rangle^{\otimes 3}$. We define $\{A_e^{(v)}\}, \{B_e\}, |\psi\rangle$ to be the ideal strategy *for the Magic Pentagram game.*

The robust self-testing theorem for the Magic Pentagram game is the following.

Theorem 7. *The Magic Pentagram game mod* 2 *self-tests the ideal strategy with perfect completeness and $O(\sqrt{\varepsilon})$-robustness.*

Again, we will only prove the exact version, and we will refer the reader to [25] for the robust version.

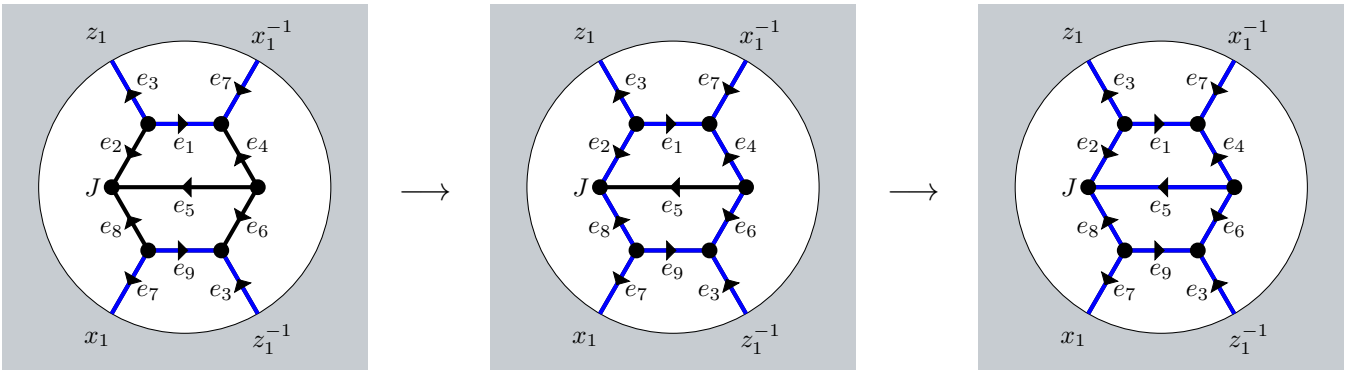


Figure 3.11: The group picture proves that $x_1 z_1 x_1^{-1} z_1^{-1} = J$ in the solution group for the magic square with the identification $x_1 = e_7, x_2 = e_9, z_1 = e_3, z_2 = e_1$. (Compare Figure 3.10.) The blue-colored edges illustrate that $\{x_1, z_1, x_2, z_2, J\}$ generates the solution group for the magic square.

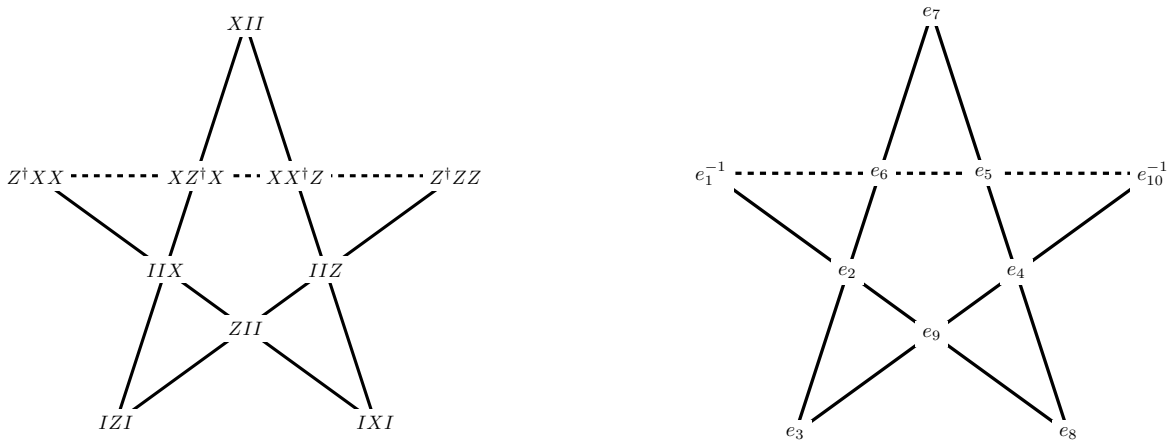


Figure 3.12: The standard operator solution for the Magic Pentagram.

Let Γ_3 be the solution group for the Magic Pentagram. The crux is again identifying Γ_3 as group of Pauli operators. We will prove the following.

Proposition 4. $\Gamma_3 \cong \mathcal{P}_2^{\otimes 3}$.

Theorem 7 follows immediately from Proposition 4, analogously to the Magic Square case.

We prove proposition 4.

Lemma 14. *The commutator subgroup* $[\Gamma_3, \Gamma_3]$ *is* $\langle J \rangle$*, the cyclic subgroup generated by* J*.*

Lemma 15. *Let* $x_1, x_2, x_3, z_1, z_2, z_3$ *be any generators of* Γ_3 *such that in the linear constraint graph, the edge pairs* $\{x_i, x_j\}, \{z_i, z_j\}, \{x_i, z_j\}, i \neq j$ *are* intersecting *(see Lemma 13), while the edge pairs* $\{x_i, z_i\}$ *are not. Then*

1. $[x_i, z_i] = J$*, and*
2. $\{x_i, z_i, J \mid i \leq 3\}$ *generates* Γ_3.

Proof. 1. If x_1 and z_1 are any pair of edges not sharing a vertex, then the group picture of Figure 3.13 establishes the twisted commutation relation. If x_i and z_i are any other pair of edges which do not share a vertex, then there is an automorphism of the graph K_5 sending $x_1 \mapsto x_i$ and $z_1 \mapsto z_i$. Therefore, we can draw the same group picture with a different labeling to prove that x_i and z_i share the same twisted commutation relation.

2. See Figure 3.13, which is interpreted the same way as Figure 3.11 from the Magic Square case. □

Figure 3.13: The leftmost group picture proves that $x_1 z_1 x_1^{-1} z_1^{-1} = J$ in Γ_3, with $x_1 = e_7, z_1 = e_9$. Identifying further $x_2 = e_8, z_2 = e_3, x_3 = e_2, z_3 = e_4$ and following the color of the edges shows that $\{x_i, z_i, J \mid i \leq 3\}$ generates Γ_3.

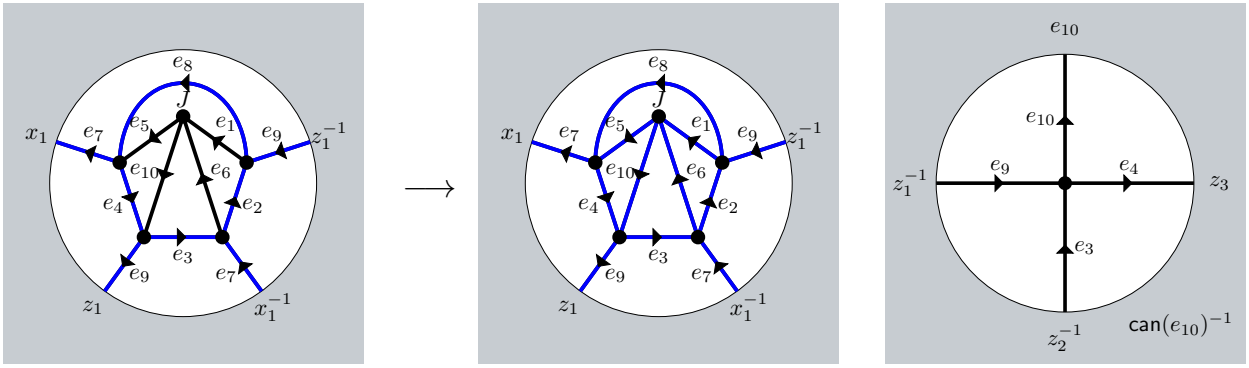


Figure 3.14: The rightmost figure is a Γ_3-picture showing $\mathsf{can}(e_{10}) = z_1 z_2 z_3^{-1}$.

We fix the identification $x_1 = e_7, z_1 = e_9, x_2 = e_8, z_2 = e_3, x_3 = e_2, z_3 = e_4$ (c.f. Figure 3.12.)

Proof of Proposition 4. As in the Magic Square case, all that remains to check is that the generators of $\mathcal{P}_2^{\otimes 3}$ satisfy the relations of Γ_3. This amounts to checking that the pentagram of operators in Figure 3.12 is a 2-dimensional Mermin Magic Pentagram in the usual sense, i.e. operators on the same line commute, the alternating products across the four solid lines are each I, and the alternating product across the dashed line is $-I$. □

Chapter 4

A CONCRETE APPLICATION: DELEGATING A QUANTUM COMPUTATION

In the previous chapter, we learnt that certain quantum correlations have the property of characterizing uniquely the quantum state and measurements that achieve them. Such states and measurements, however, are certainly not arbitrary and a given self-testing correlation certifies a very *specific* setup. In this chapter, we investigate the question of whether and how the self-tests described in Chapter 3 can be exploited or augmented to allow a classical verifier to orchestrate an arbitrary full-fledged quantum computation.

Organization In Section 4.1, we give an overview of the problem and of our solution. In Section 4.2, we give an informal overview of our main technical contribution, a robust self-test for products of single-qubit Clifford observables on many EPR pairs. We then set up the formal notation for the next two sections. In Section 4.3, we describe the Pauli Braiding test of Natarajan and Vidick [69] which allows to test products of Pauli X and Z measurements. In Section 4.4, we extend this test first to account for Pauli Y measurements, and then to account for any single-qubit Clifford observable. In Section 4.5, we describe our delegation protocols and prove their completeness and soundness.

4.1 Introduction

For the foreseeable future, making use of a quantum computer will likely require delegating the computation to a potentially untrusted cloud service, such as that of IBM [48]. Recent progress towards implementing limited quantum computers has added urgency to the already important question of how a classical verifier can test the correctness of the computations she delegates. In this chapter, we will investigate this question by making one crucial assumption on the system to be tested: that it consists of two spatially isolated components that are unable to communicate throughout the experiment. This will allows us to exploit some of the self-testing theory developed in Chapter 3. Certainly, two things seem essential in order for self-testing results to be helpful in verifiably delegating a quantum computation:

- They should be robust, in the sense that close-to-optimal correlations, should still allow us to conclude that the quantum apparatus under study is close to the ideal apparatus (see Definition 9 for a formal definition). This is essential because in practice one never "observes" an optimal winning probability, but one can only make statements up to some statistical confidence.
- They should be applicable to higher-dimensional states, not just one or two EPR pairs, but potentially many copies.

For the first question, the results of [62] and [82] showed that the CHSH game provides a robust self-test of a single EPR pair, wherein an ϵ-close to optimal winning probability requires an $O(\sqrt{\epsilon})$-close to optimal state. For the second question, the most natural approach to certifying many EPR pairs is to repeat the CHSH game *sequentially* and requiring that the players win a high-enough fraction of the games played. In 2012, Reichardt, Unger and Vazirani proved a robust self-testing theorem for playing a sequence of n CHSH games [82]. The main technical difficulty that needs to be overcome to prove such a result is to establish a tensor product structure in the provers' registers, in spite of the fact that they might try to correlate their answers for a certain round with their questions and answers from previous rounds. The sequential test of [82] is not a non-local game in the traditional sense, since there is more than one round of interaction between the verifier and the players. Nonetheless, the result showed that the only way for the players to play optimally in the n-sequentially repeated CHSH game is to be making certain Pauli X and Z measurements on a state that is close to n EPR pairs. Aside from its intrinsic interest, this theorem had two important consequences. One was the first device-independent protocol for quantum key distribution. The second was a protocol whereby a completely classical verifier can test a universal quantum computer consisting of two spatially isolated devices. The resulting protocol for delegating quantum computations has received a lot of attention as the first classical-verifier

delegation protocol. We believe that this attention is especially justified in light of the current race for building a quantum computer and the recent experimental advances.

Unfortunately, the complexity overhead of the delegation protocol from [82], in terms of both the number of EPR pairs needed for the provers and the overall time complexity of the provers as well as the (classical) verifier, while polynomial, is prohibitively large. Although the authors of [82] do not provide an explicit value for the exponent, in [44] it is estimated that their protocol requires resources that scale like $\Omega(g^{8192})$, where g is the number of gates in the delegated circuit (notwithstanding the implicit constant, this already makes the approach thoroughly impractical for even a 2-gate circuit!). The large overhead is in part due to a very small (although still inverse polynomial) gap between the completeness and soundness parameters of the rigidity theorem; this requires the verifier to perform many more Bell tests than the actual number of EPR pairs needed to implement the computation, which would scale linearly with the circuit size.

Subsequent work has presented significantly more efficient protocols for achieving the same, or similar, functionality [59, 40, 44]. We refer to Table 4.1 for a summary of our estimated lower bounds on the complexity of each of these results (not all papers provide explicit bounds, in which case our estimates, although generally conservative, should be taken with caution). Prior to our work, the best two-prover delegation protocol required resources scaling like g^{2048} for delegating a g-gate circuit. Things improve significantly if we allow for more than two provers, however, the most efficient multi-prover delegation protocols still required resources that scale as at least $\Omega(g^4 \log g)$ for delegating a g-gate circuit on n qubits. Since we expect that in the foreseeable future most quantum computations will be delegated to a third-party server, even such small polynomial overhead is unacceptable, as it already negates the quantum advantage for a number of problems, such as quantum search.

The most efficient classical-verifier delegation protocols known [36, 69], with $\mathrm{poly}(n)$ and 7 provers, respectively, require resources that scale as $O(g^3)$, but this efficiency comes at the cost of a technique of "post-hoc" verification. In this technique, the provers must learn the verifier's input even before they are separated, so that they can prepare the history state for the computation.[1] As a result, these protocols are not blind[2]. Moreover, while the method does provide a means for verifying the outcome of an arbitrary quantum computation, in contrast to [82] it does not provide a means for the verifier to test the provers' implementation of the required circuit on a gate-by-gate basis. Other works, such as [45], achieve two-prover verifiable delegation with complexity that scales like $O(g^4 \log g)$, but in much weaker models; for example, in [45] the provers' private system

[1] Using results of Ji [49], this allows the protocol to be single-round. Alternatively, the state can be created by a single prover and teleported to the others with the help of the verifier, resulting in a two-round protocol.

[2] *Blindness* is a property of delegation protocols, which informally states that the prover learns nothing about the verifier's private circuit.

is assumed a priori to be in tensor product form, with well-defined registers. General techniques are available to remove the strong assumption, but they would lead to similar large overhead as previous results.

In contrast, in the setting where the verifier is allowed some limited quantum power, such as the ability to generate single-qubit states and measure them with observables from a small finite set, efficient schemes for blind verifiable delegation do exist. In this case, only a single prover is needed [3, 37, 65, 11, 46, 66, 39, 67] (see also [35] for a recent survey), and the most efficient *single-prover quantum-verifier* protocols can evaluate a quantum circuit with g gates in time $O(g)$. The main reason these protocols are much more efficient than the classical-verifier multi-prover protocols is that they avoid the need for directly testing any of the qubits used by the prover, instead requiring the trusted verifier to directly either prepare or measure the qubits used for the computation.

New rigidity results We overcome the efficiency limitations of multi-prover delegation protocols by introducing a new robust rigidity theorem. Our theorem allows a classical verifier to certify (in parallel as opposed to in sequence) that two non-communicating provers apply a measurement associated with an arbitrary m-qubit tensor product of single-qubit Clifford observables on their respective halves of m shared EPR pairs. This is the first result to achieve self-testing for such a large class of measurements. The majority of previous works in self-testing have been primarily concerned with certifying the state and were limited to simple single-qubit measurements in the X-Z plane. Prior self-testing results for multi-qubit measurements only allow to test for tensor products of σ_X and σ_Z observables. While this is sufficient for verification in the post-hoc model of [36], testing for σ_X and σ_Z observables does not directly allow for the verification of a general computation (unless one relies on techniques such as process tomography [82], which introduce substantial additional overhead).

Our first contribution is to extend the "Pauli Braiding test" of [69], which allows to test tensor products of σ_X and σ_Z observables with constant robustness, to allow for σ_Y observables as well. This is somewhat subtle due to an ambiguity in the complex phase that cannot be detected by any classical two-player test; we formalize the ambiguity and show how it can be effectively accounted for. Our second contribution is to substantially increase the set of elementary gates that can be tested, to include arbitrary m-qubit tensor products of single-qubit Clifford observables. This is achieved by introducing a new "conjugation test", which tests how an observable applied by the provers acts on the Pauli group. The test is inspired by general results of Slofstra [90], but is substantially more direct.

A key feature of our rigidity results is that their robustness scales independently of the number of EPR pairs tested, as in [69]. This is crucial for the efficiency of our delegation protocols. The

robustness for previous results in parallel self-testing typically had a polynomial dependence on the number of EPR pairs tested. We give an informal statement of our robust rigidity theorem.

Theorem 8 (Informal)**.** *Let $m \in \mathbb{Z}_{>0}$. Let $\mathcal{G}$ be a fixed, finite set of single-qubit Clifford observables. Then there exists an efficient two-prover test $\textsc{rigid}(\mathcal{G}, m)$ with $O(m)$-bit questions (a constant fraction of which are of the form $W \in \mathcal{G}^m$) and answers such that the following properties hold:*

- *(Completeness) There is a strategy for the provers that uses $m+1$ EPR pairs and succeeds with probability at least $1 - e^{-\Omega(m)}$ in the test.*
- *(Soundness) For any $\varepsilon > 0$, any strategy for the provers that succeeds with probability $1-\varepsilon$ in the test must be $\mathrm{poly}(\varepsilon)$-close, up to local isometries, to a strategy in which the provers begin with $(m+1)$ EPR pairs and is such that upon receipt of a question of the form $W \in \mathcal{G}^m$ the prover measures the "correct" observable W.*

Although we do not strive to obtain the best dependence on ε, we believe it should be possible to obtain a scaling of the form $C\sqrt{\varepsilon}$ for a reasonable constant C. We give a detailed overview of the test in Section 4.4.

New delegation protocols We employ the new rigidity theorem to obtain two new efficient two-prover classical-verifier protocols in which the complexity of verifiably delegating a g-gate quantum circuit scales as $O(g \log g)$.[3]

We achieve our protocols by adapting the efficient single-prover quantum-verifier delegation protocol introduced by Broadbent [11] (we refer to this as the "EPR protocol"), which has the advantage of offering a direct implementation of the delegated circuit, in the circuit model of computation and with very little modification needed to ensure verifiability, as well as a relatively simple and intuitive analysis.

Our first protocol is blind, and requires a number of rounds of interaction that scales linearly with the depth of the circuit being delegated. The second protocol is not blind, but only requires a constant number of rounds of interaction with the provers. Our work is the first to propose verifiable two-prover delegation protocols which overcome the prohibitively large resource requirements of all previous multi-prover protocols, requiring only a quasilinear amount of resources, in terms of

[3]The $\log g$ overhead is due to the complexity of sampling from the right distribution in rigidity tests. We leave the possibility of removing this by derandomization for future work. Another source of overhead is in achieving blindness: in order to hide the circuit, we encode it as part of the input to a universal circuit, introducing a factor of $O(\log g)$ overhead.

number of EPR pairs and time. However, notwithstanding our improvements, a physical implementation of verifiable delegation protocols remains a challenging task for the presently available technology.

We introduce the protocols in more detail. The protocols provide different methods to delegate the quantum computation performed by the quantum verifier from [11] to a second prover (call him PV for Prover V). The rigidity test is used to verify that the second prover indeed performs the same actions as the honest verifier, which are sequences of single-qubit measurements of Clifford observables from the set $\Sigma = \{X, Y, Z, F, G\}$ (where F and G are defined in (4.2)).

In the first protocol, one of the provers plays the role of Broadbent's prover (call him PP for Prover P), and the other plays the role of Broadbent's verifier (we refer to this as PV). The protocol is divided into two sub-games; which game is played is chosen by the verifier by flipping a biased coin with appropriately chosen probabilities.

- The first game is a sequential version of the rigidity game $\textsc{rigid}(\Sigma, m)$ (from Theorem 8) described in Figure 4.21. This aims to enforce that PV performs precisely the right measurements;
- The second game is the delegation game, described in Figures 4.18, 4.19, and 4.20, and whose structure is summarized in Figure 4.16. Here the verifier guides PP through the computation in a similar way as in the EPR Protocol.

We remark that in both sub-games, the questions received by PV are of the form $W \in \Sigma^m$, where $\Sigma = \{X, Y, Z, F, G\}$ is the set of measurements performed by the verifier in Broadbent's EPR protocol. The questions for PV in the two sub-games are sampled from the same distribution. This ensures that PV is not able to tell which kind of game is being played. Hence, we can use our rigidity result of Theorem 8 to guarantee honest behavior of PV in the delegation sub-game. We call this protocol *Verifier-on-a-Leash Protocol*, or "leash protocol" for short.

The protocol requires $(2d + 1)$ rounds of interaction, where d is the depth of the circuit being delegated (see Section 4.5.1.2 for a precise definition of how this is computed). The protocol requires $O(n + g)$ EPR pairs to delegate a g-gate circuit on n qubits, and the overall time complexity of the protocol is $O(g \log g)$. The input to the circuit is hidden from the provers, meaning that the protocol can be made blind by encoding the circuit in the input, and delegating a universal circuit.

The completeness of the protocol follows directly from the completeness of [11]. Once we ensure the correct behavior of PV using our rigidity test, soundness follows from [11] as well, since the combined behavior of our verifier and an honest PV is nearly identical to that of Broadbent's verifier.

The second protocol also starts from Broadbent's protocol, but modifies it in a different way to achieve a protocol that only requires a constant number of rounds of interaction. The proof of security is slightly more involved, but the key ideas are the same: we use a combination of our new self-testing results and the techniques of Broadbent's protocol to control the two provers, one of which plays the role of Broadbent's verifier, and the other the role of the prover. Because of the more complicated "leash" structure in this protocol, we call it the *Dog-Walker Protocol*. Like the leash protocol, the Dog-Walker Protocol has overall time complexity $O(g \log g)$. Unlike the leash protocol, the Dog-Walker protocol is not blind. In particular, while PV and PP would have to collude after the protocol is terminated to learn the input in the leash protocol, in the Dog-Walker protocol, PV simply receives the input in clear.

Based on the Dog-Walker Protocol, it is possible to design a classical-verifier two-prover protocol for all languages in QMA. This is achieved along the same lines as the proof that QMIP = MIP* from [82]. The first prover, given the input, creates the QMA witness and teleports it to the second prover with the help of the verifier. The verifier then delegates the verification circuit to the second prover, as in the Dog-Walker Protocol; the first prover can be re-used to verify the operations of the second one.

Related work and directions for future work We have introduced a new rigidity theorem and shown how it can be used to transform a specific quantum-verifier delegation protocol, due to Broadbent, into a classical-verifier protocol with an additional prover, while suffering very little overhead in terms of the efficiency of the protocol. We believe that a similar transformation could be performed starting from delegation protocols based on other models of computation, such as the protocol in the measurement-based model of [37] or the protocol based on computation by teleportation considered in [82], and would lead to similar efficiency improvements.

Recently, [47] provided an experimental demonstration of a two-prover delegation protocol based on [82] for a 3-qubit quantum circuit based on Shor's algorithm to factor the number 15; in order to obtain an actual implementation, necessitating "only" on the order of 6000 CHSH tests, the authors had to make the strong assumption that the devices behave in an i.i.d. manner at each use, and could not use the most general testing results from [82]. We believe that our improved rigidity theorem could lead to an implementation that does not require any additional assumption.

We note that both our protocols require the verifier to communicate with one prover after at least one round of communication with the other has been completed. This means that the requirement that the two provers do not communicate throughout the protocol cannot be enforced through space-like separation, and should rather be taken as an a priori assumption. Since the protocol of [42] is not blind, it is still an important open question whether there exists a multi-prover delegation protocol

that consists of a single round of simultaneous communication with each prover, and is both blind and verifiable. A different avenue to achieve this is to forego information-theoretic security, and rely on computational assumptions on the power of the provers to achieve protocols with more properties (single-server, non-interactive, blind) [31, 4, 54, 55]. In particular, in a recent breakthrough result [55], Mahadev showed that a classical-verifier can verifiably delegate her computation to a *single* computationally bounded quantum prover (albeit not necessarily in a truly efficient manner).

Finally, due to its efficiency and robustness, our ridigity theorem is a potentially useful tool in many other cryptographic protocols. For instance, an interesting direction to explore is the possibility of exploiting our theorem to achieve more efficient protocols for device-independent quantum key distribution, entanglement certification or other cryptographic protocols involving more complex untrusted computation of the users, in parallel.

	Provers	Rounds	Total Resources	Blind
RUV 2012 [82]	2	$\mathrm{poly}(n)$	$\geq g^{8192}$	yes
McKague 2013 [59]	$\mathrm{poly}(n)$	$\mathrm{poly}(n)$	$\geq 2^{153} g^{22}$	yes
GKW 2015 [40]	2	$\mathrm{poly}(n)$	$\geq g^{2048}$	yes
HDF 2015 [44]	$\mathrm{poly}(n)$	$\mathrm{poly}(n)$	$\Theta(g^4 \log g)$	yes
Verifier-on-a-Leash Protocol (Section 4.5.2)	2	$O(\mathrm{depth})$	$\Theta(g \log g)$	yes
Dog-Walker Protocol (Section 4.5.3)	2	$O(1)$	$\Theta(g \log g)$	no

Table 4.1: Resource requirements of various delegation protocols in the multi-prover model. We use n to denote the number of qubits and g the number of gates in the delegated circuit. "depth" refers to the depth of the delegated circuit. "Total Resources" refers to the gate complexity of the provers, the number of EPR pairs of entanglement needed, and the number of bits of communication in the protocol. To ensure fair comparison, we require of each protocol that it produces the correct answer with probability 99%. For all protocols except our two new protocols, this requires a polynomial number of sequential repetitions, which is taken into account when computing the total resources.

4.2 Robust self-testing in parallel

In this section, we give an overview of our robust self-test, and we establish some notation.

Each of our delegation protocols includes a self-test, or *rigidity test* that is meant to verify that one of the provers measures his half of shared EPR pairs in a basis specified by the verifier, thereby preparing one of a specific family of post-measurement states on the other prover's space; the post-measurement states will form the basis for the delegated computation. This will be used to certify that one of the provers in our two-prover schemes essentially behaves as the quantum part of the verifier in Broadbent's EPR protocol.

The main rigidity game is given in Section 4.4.3, while Sections 4.4.4 and 4.4.5 contain variants of it, which we later employ in the Leash and Dog-Walker protocols; here we give a brief overview of the structure of the test. The test is parametrized by the number m of EPR pairs to be used. The test $\textsc{cliff}(\Sigma, m)$ is a single round of classical interaction between the verifier and the two provers. With constant probability the verifier sends one of the provers a string W chosen uniformly at random from Σ^m where the set $\Sigma = \{X, Y, Z, F, G\}$ contains a label for each single-qubit observable to be tested. With the remaining probability other queries, requiring the measurement of observables not in Σ^m (such as the measurement of pairs of qubits in the Bell basis).

In general, an arbitrary strategy for the provers in the rigidity game consists of an arbitrary entangled state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ (which we take to be pure), and measurements (which we take to be projective) for each possible question.[4] This includes an m-bit outcome projective measurement $\{W^u\}_{u\in\{0,1\}^m}$ for each of the queries $W \in \Sigma^m$. Our rigidity result states that any strategy that succeeds with probability $1-\varepsilon$ in the test is within $\mathrm{poly}(\varepsilon)$ of the honest strategy, up to local isometries (see Theorem 9 for a precise statement). This is almost true, but for an irreconcilable ambiguity in the definition of the complex phase $\sqrt{-1}$. The fact that complex conjugation of observables leaves correlations invariant implies that no classical test can distinguish between the two nontrivial inequivalent irreducible representations of the Pauli group, which are given by the Pauli matrices $\sigma_X, \sigma_Y, \sigma_Z$ and their complex conjugates $\overline{\sigma_X} = \sigma_X, \overline{\sigma_Z} = \sigma_Z, \overline{\sigma_Y} = -\sigma_Y$ respectively. In particular, the provers may use a strategy that uses a combination of both representations; as long as they do so consistently, no test will be able to detect this behavior.[5]. The formulation of our result accommodates this irreducible degree of freedom by forcing the provers to use a single qubit, the $(m+1)$-st, to make their choice of representation (so honest provers require the use of $(m+1)$ EPR pairs to test the operation of m-fold tensor products of observables from Σ, acting on m EPR

[4] We make the assumption that the players employ a pure-state strategy for convenience, but it is easy to check that all proofs extend to the case of a mixed strategy. Moreover, it is always possible to consider (as we do) projective strategies only by applying Naimark's dilation theorem, and adding an auxiliary local system to each player as necessary, since no bound is assumed on the dimension of their systems.

[5] See [82, Appendix A] for an extended discussion of this issue, with a similar resolution to ours.

pairs).

We introduce here the language required to formulate our testing results in Section 4.4.

4.2.1 Testing

In this section, we recall some standard notions, which we use throughout the chapter, including state-dependent distance measure, local isometries, etc. We also introduce a framework of "tests for relations" that will be convenient to formulate our results.

4.2.1.1 Distance measures

Ultimately our goal is to test that a player implements a certain tensor product of single-qubit or two-qubit measurements defined by observables such as σ_X, σ_Y, or σ_G. Since it is impossible to detect whether a player applies a certain operation X on state $|\psi\rangle$, or $VXV^\dagger$ on state $V|\psi\rangle$, for any isometry $V : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ such that $V^\dagger V = \mathbb{1}$, we will (as is standard in testing) focus on testing identity up to *local isometries*. Towards this, we introduce the following important piece of notation:

Definition 29. *For finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_{A'}$, $\delta > 0$, and operators $R \in \mathrm{L}(\mathcal{H}_A)$ and $S \in \mathrm{L}(\mathcal{H}_{A'})$ we say that R and S are δ-isometric with respect to $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and write $R \simeq_\delta S$, if there exists an isometry $V : \mathcal{H}_A \to \mathcal{H}_{A'}$ such that*

$$\left\| (R - V^\dagger S V) \otimes \mathbb{1}_B |\psi\rangle \right\|^2 = O(\delta) .$$

If V is the identity, then we further say that R and S are δ-equivalent, and write $R \approx_\delta S$ for $\|(R - S) \otimes \mathbb{1}_B |\psi\rangle\|^2 = O(\delta)$.

The notation $R \simeq_\delta S$ carries some ambiguity, as it does not specify the state $|\psi\rangle$. The latter should always be clear from context: we will often simply write that R and S are δ-isometric, without explicitly specifying $|\psi\rangle$ or the isometry. The relation is transitive, but not reflexive: the operator on the right will always act on a space of dimension at least as large as that on which the operator on the left acts. The notion of δ-equivalence is both transitive (its square root obeys the triangle inequality) and reflexive, and we will use it as our main notion of distance.

4.2.1.2 Tests

We formulate our tests as two-player games in which both players are treated symmetrically. We often use the same symbol, a capital letter $X, Z, W, \ldots$, to denote a question in the game and the associated projective measurement $\{W^a\}$ applied by the player upon receipt of that question. To a projective measurement with outcomes in $\{0,1\}^n$ we associate a family of observables $W(u)$

parametrized by n-bit strings $u \in \{0,1\}^n$, defined by $W(u) = \sum_a (-1)^{u\cdot a} W^a$. If $n = 1$ we simply write $W = W(1) = W^0 - W^1$; note that $W(0) = \mathbb{1}$.

With the exception of the Tomography Test TOM presented in Section 4.4.5, all the games, or tests, we consider implicitly include a "consistency test" which is meant to enforce that whenever both players are sent identical questions, they produce matching answers. More precisely, let T be any of the two-player tests described in the paper. Let $\Pr_T(W, W')$ be the distribution on questions (W, W') to the players that is specified by T. Since the players are always treated symmetrically, $\Pr_T(\cdot,\cdot)$ is permutation-invariant. Let $\Pr_T(\cdot)$ denote the marginal on either player. Then, instead of executing the test T as described, the verifier performs the following:

(i) With probability $1/2$, execute T.

(ii) With probability $1/2$, select a random question W according to $\Pr_T(W)$. Send W to both players. Accept if and only if the players' answers are equal.

Then, success with probability at least $1-\varepsilon$ in the modified test implies success with probability at least $1-2\varepsilon$ in the original test, as well as in the consistency test. If $\{W^a_{\mathsf{A}}\}$ and $\{W^b_{\mathsf{B}}\}$ are the players' corresponding projective measurements, the latter condition implies

$$\begin{aligned}\sum_a \| (W^a_{\mathsf{A}} \otimes \mathbb{1} - \mathbb{1} \otimes W^a_{\mathsf{B}}) \, |\psi\rangle_{\mathsf{AB}} \|^2 &= 2 - 2 \sum_a \langle \psi | \, W^a_{\mathsf{A}} \otimes W^a_{\mathsf{B}} \, |\psi\rangle \\ &\leq 4\varepsilon \,, \end{aligned} \tag{4.1}$$

so that $W^a_{\mathsf{A}} \otimes \mathbb{1} \approx_\varepsilon \mathbb{1} \otimes W^a_{\mathsf{B}}$ (where the condition should be interpreted on average over the choice of a question W distributed as in the test). Similarly, if W_{A}, W_{B} are observables for the players that succeed in the consistency test with probability $1-2\varepsilon$ we obtain $W_{\mathsf{A}} \otimes \mathbb{1} \approx_\varepsilon \mathbb{1} \otimes W_{\mathsf{B}}$. We will often use both relations to "switch" operators from one player's space to the other's; as a result we will also often omit an explicit specification of which player's space an observable is applied to.

4.2.1.3 Strategies

Given a two-player game, or test, a strategy for the players consists of a bipartite entangled state $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ together with families of projective measurements $\{W^a_{\mathsf{A}}\}$ for Alice and $\{W^a_{\mathsf{B}}\}$ for Bob, one for each question W that can be sent to either player in the test. As already mentioned, for convenience we restrict our attention to pure-state strategies employing projective measurements. We will loosely refer to a strategy for the players as $(W, |\psi\rangle)$, with the symbol W referring to the complete set of projective measurements used by the players in the game; taking advantage of symmetry we often omit the subscript A or B, as all statements involving observables for one player hold verbatim with the other player's observables as well.

4.2.1.4 Relations

We use $\mathcal{R}$ to denote a set of relations over variables $X, Z, W, \ldots$, such as

$$\mathcal{R} = \left\{ XZXZ = -\mathbb{1},\ HX = ZH,\ X, Z, H \in \mathrm{Obs} \right\}.$$

We only consider relations that can be brought in the form either $f(W) = (-1)^a W_1 \cdots W_k = \mathbb{1}$, where the W_i are (not necessarily distinct) unitary variables and $a \in \mathbb{Z}_2$, or $f(W) = W_1 \cdot (\sum_a \omega_a W_2^a) = \mathbb{1}$, where W_1 is a unitary variable, $\{W_2^a\}$ a projective measurement with s possible outcomes, and ω_a are (arbitrary) s-th roots of unity.

Definition 30 (Rigid self-test)**.** *We say that a set of relations $\mathcal{R}$ is $(c, \delta(\varepsilon))$-testable, on average under the distribution $\mathcal{D} : \mathcal{R} \to [0,1]$, if there exists a game (or test) G with question set $\mathcal{Q}$ that includes (at least) a symbol for each variable in $\mathcal{R}$ that is either an observable or a POVM and such that:*

- *(*Completeness*) There exists a set of operators which exactly satisfy all relations in $\mathcal{R}$ and a strategy for the players which uses these operators (together possibly with others for the additional questions) that has success probability at least c;*
- *(*Soundness*) For any $\varepsilon > 0$ and any strategy $(W, |\psi\rangle_{AB})$ that succeeds in the game with probability at least $c - \varepsilon$, the associated measurement operators satisfy the relations in $\mathcal{R}$ up to $\delta(\varepsilon)$, in the state-dependent norm. More precisely, on average over the choice of a relation $f(W) = \mathbb{1}$ from $\mathcal{R}$ chosen according to $\mathcal{D}$, it holds that $\| \mathbb{1} \otimes (f(W) - \mathbb{1}) |\psi\rangle_{AB} \|^2 \leq \delta(\varepsilon)$.*

If both conditions hold, we also say that the game G is a robust $(c, \delta(\varepsilon))$ self-test for the relations $\mathcal{R}$.

Most of the games we consider have perfect completeness, $c = 1$, in which case we omit explicitly mentioning the parameter. The distribution $\mathcal{D}$ will often be implicit from context, and we do not always specify it explicitly (e.g. in case we only measure $\delta(\varepsilon)$ up to multiplicative factors of order $|\mathcal{R}|$ the exact distribution $\mathcal{D}$ does not matter as long as it has complete support).

Definition 31 (Stable relations)**.** *We say that a set of relations $\mathcal{R}$ is $\delta(\varepsilon)$-stable, on average under the distribution $\mathcal{D} : \mathcal{R} \to [0,1]$, if for any two families of operators $W_A \in \mathrm{L}(\mathcal{H}_A)$ and $W_B \in \mathrm{L}(\mathcal{H}_B)$ that are consistent on average, i.e.*

$$\mathbb{E}_{f \sim \mathcal{D}} \mathbb{E}_{W \in uf} \left\| (\mathbb{1} \otimes W_B - W_A \otimes \mathbb{1}) |\psi\rangle \right\|^2 \leq \varepsilon,$$

where $W \in_U f$ is shorthand for W being a uniformly random operator among those appearing in the relation specified by f, and satisfy the relations on average, i.e.

$$\mathop{\mathbb{E}}_{\substack{f\sim\mathcal{D}:\\ f(W)=\mathbb{1}\in\mathcal{R}}} \left\| (f(W_A) - \mathbb{1}) \otimes \mathbb{1} \, |\psi\rangle \right\|^2 \leq \varepsilon \,,$$

there exists operators $\hat{W}$ which satisfy the same relations exactly and are $\delta(\varepsilon)$-isometric to the W with respect to $|\psi\rangle$, on average over the choice of a random relation in $\mathcal{R}$ and a uniformly random W appearing in the relation, i.e. there exists an isometry V_A such that

$$\mathbb{E}_{f\sim\mathcal{D}} \mathbb{E}_{W\in_U f} \left\| (\hat{W}_A - V_A^\dagger W_A V_A) \otimes \mathbb{1} \, |\psi\rangle \right\|^2 = O(\delta(\varepsilon)) \,.$$

4.2.2 Some simple tests

4.2.2.1 Notation

We often write $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$ for a string of bits, and $W = W_1 \cdots W_m \in \Sigma^m$ for a string, where Σ is a finite alphabet. If $S \subseteq \{1, \ldots, m\}$ we write W_S for the sub-string of W indexed by S. For an event E, we use 1_E to denote the indicator variable for that event, so $1_E = 1$ if E is true, and otherwise $1_E = 0$.

4.2.2.2 Observables.

We use capital letters $X, Z, W, \ldots$ to denote observables. We use greek letters σ, τ with a subscript σ_W, τ_W, to emphasize that the observable W specified as subscript acts in a particular basis. For example, X is an arbitrary observable but σ_X is specifically the Pauli X matrix defined in (2.1).

For $a \in \{0,1\}^n$ and commuting observables $\sigma_{W_1}, \ldots, \sigma_{W_n}$, we write $\sigma_W(a) = \prod_{i=1}^n (\sigma_{W_i})^{a_i}$. The associated projective measurements are $\sigma_{W_i} = \sigma^0_{W_i} - \sigma^1_{W_i}$ and $\sigma^u_W = \mathbb{E} a (-1)^{u\cdot a} \sigma_W(a)$. Often the σ_{W_i} will be single-qubit observables acting on distinct qubits, in which case each is implicitly tensored with identity outside of the qubit on which it acts.

4.2.2.3 Pauli and Clifford groups.

The single-qubit Weyl-Heisenberg group

$$\mathcal{H}^{(1)} = H(\mathbb{Z}_2) = \left\{ (-1)^c \sigma_X(a) \sigma_Z(b),\, a, b, c \in \{0,1\} \right\}$$

is the matrix group generated by the Pauli σ_X and σ_Z. We let $\mathcal{H}^{(n)} = H(\mathbb{Z}_2^n)$ be the direct product of n copies of $\mathcal{H}^{(1)}$. The n-qubit Clifford group is the normalizer of $\mathcal{H}^{(n)}$ in the unitary group, up to phase:

$$G_{\mathcal{C}}^{(n)} = \left\{ G \in \mathrm{U}((\mathbb{C}^2)^{\otimes n}) : \, G\sigma G^\dagger \in \mathcal{H}^{(n)} \quad \forall \sigma \in \mathcal{H}^{(n)} \right\}.$$

Some Clifford observables we will use include

$$\sigma_H = \frac{\sigma_X + \sigma_Z}{\sqrt{2}}, \qquad \sigma_{H'} = \frac{\sigma_X - \sigma_Z}{\sqrt{2}}, \qquad \sigma_F = \frac{-\sigma_X + \sigma_Y}{\sqrt{2}}, \qquad \sigma_G = \frac{\sigma_X + \sigma_Y}{\sqrt{2}}. \tag{4.2}$$

Note that σ_H and $\sigma_{H'}$ are characterized by $\sigma_X \sigma_H \sigma_X = \sigma_{H'}$ and $\sigma_Z \sigma_H \sigma_Z = -\sigma_{H'}$. Similarly, σ_F and σ_G are characterized by $\sigma_X \sigma_F \sigma_X = -\sigma_G$ and $\sigma_Y \sigma_F \sigma_Y = \sigma_G$.

4.2.2.4 The Magic Square game

We have already encountered the Magic Square game in Section 3.5. We will use the Magic Square game as a building block for more complex tests in the next sections, noting that it provides a robust self-test test for the two-qubit Weyl-Heisenberg group (see Section 4.2.2.1 for the definition). We recall the game here for convenience. Questions are specified by a triple of labels corresponding to the same row or column from the square pictured in Figure 4.1 (so a typical question could be (IZ, XI, XZ); there are 6 questions in total, each a triple). An answer is composed of three values in $\{\pm 1\}$, one for each of the labels making up the question. Answers from the prover should be entrywise consistent, and such that the product of the answers associated to any row or column except the last should be $+1$; for the last column it should be -1. The labels indicate the "honest" strategy for the game, which consists of each prover measuring two half-EPR pairs using the commuting Pauli observables indicated by the labels of his question.

IZ	ZI	ZZ
XI	IX	XX
XZ	ZX	YY

Figure 4.1: Questions, and a strategy, for the Magic Square game

The following lemma states some properties of the Magic Square game, interpreted as a self-test (see e.g. [100]).

Lemma 16. *Suppose a strategy for the provers, using state $|\psi\rangle$ and observables W, succeeds with probability at least $1-\varepsilon$ in the Magic Square game. Then there exist isometries $V_D : \mathcal{H}_D \to (\mathbb{C}^2 \otimes \mathbb{C}^2)_{D'} \otimes \mathcal{H}_{\hat{D}}$, for $D \in \{A, B\}$ and a state $|AUX\rangle_{\hat{A}\hat{B}} \in \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{\hat{B}}$ such that*

$$\left\| (V_A \otimes V_B) |\psi\rangle_{AB} - |EPR\rangle_{A'B'}^{\otimes 2} |AUX\rangle_{\hat{A}\hat{B}} \right\|^2 = O(\sqrt{\varepsilon}),$$

and for $W \in \{I, X, Z\}^2 \cup \{YY\}$,

$$\left\| \left(W - V_A^\dagger \sigma_W V_A\right) \otimes \mathbb{1}_B |\psi\rangle \right\|^2 = O(\sqrt{\varepsilon}).$$

4.3 The Pauli Braiding test

In this section, we review the Pauli Braiding test from Natarajan and Vidick [69], which tests products of Pauli X and Z measurements on many EPR pairs.

We start with some elementary tests, and we build up to the Pauli Braiding test. Our treatment is quite detailed but we do not provide the full proofs. We refer to [69] for a fully detailed analysis.

More precisely, in Subsection 4.3.1, we review some elementary tests whose analysis is immediate. In Subsection 4.3.2, we formulate a simple test for measurements in the Bell basis and the associated two-qubit SWAP observable. In Subsection 4.3.3, we describe (a slight extension of) the Pauli Braiding test of [69].

4.3.1 Elementary tests

Figure 4.2 summarizes some elementary tests. For each test, "Inputs" refers to a subset of designated questions in the test; "Relation" indicates a relation that the test aims to certify (in the sense of Section 4.2.1); "Test" describes the certification protocol. (Recall that all our protocols implicitly include a "consistency" test in which a question is chosen uniformly at random from the marginal distribution and sent to both provers, whose answers are accepted if and only if they are equal.)

Test $\textsc{id}(A, B)$:

- Inputs: A, B two observables on the same space $\mathcal{H}$.
- Relation: $A = B$.
- Test: Send $W \in \{A, B\}$ and $W' \in \{A, B\}$, chosen uniformly at random, to the first and second prover respectively. Receive an answer in $\{\pm 1\}$ from each prover. Accept if and only if the answers are equal whenever the questions are identical.

Test $\textsc{ac}(X, Z)$:

- Inputs: X, Z two observables on the same space $\mathcal{H}$.
- Relation: $XZ = -ZX$.
- Test: Execute the Magic Square game, using the label "X" for the "XI" query, and "Z" for the "ZI" query.

Test $\textsc{com}(A, B)$:

- Inputs: A, B two observables on the same space $\mathcal{H}$.
- Relation: $AB = BA$.
- Test: Send $W \in \{A, B\}$ chosen uniformly at random to the first prover. Send (A, B) to the second prover. Receive a bit $c \in \{\pm 1\}$ from the first prover, and two bits $(a', b') \in \{\pm 1\}^2$ from the second. Accept if and only if $c = a'$ if $W = A$, and $c = b'$ if $W = B$.

Test $\textsc{prod}(A, B, C)$:

- Inputs: A, B and C three observables on the same space $\mathcal{H}$.
- Relations: $AB = BA = C$.
- Test: Similar to the commutation game, but use C to label the question (A, B).

Figure 4.2: Some elementary tests.

Lemma 17. *Each of the tests described in Figure 4.2 is a robust $(1, \delta)$ self-test for the indicated relation(s), for some $\delta = O(\varepsilon^{1/2})$.*

Proof. The proof for each test is similar. As an example we give it for the commutation test $\textsc{com}(A, B)$.

First we verify completeness. Let A, B be two commuting observables on $\mathcal{H}_\mathsf{A} = \mathcal{H}_\mathsf{B} = \mathcal{H}$, and $|\mathrm{EPR}\rangle_{\mathsf{AB}}$ the maximally entangled state in $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. Upon receiving question A or B, the prover

measures the corresponding observable. If the question is (A, B), he jointly measures A and B. This strategy succeeds with probability 1 in the test.

Next we establish soundness. Let $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ be a state shared by the provers, A, B their observables on questions A, B, and $\{C^{a,b}\}$ the four-outcome PVM applied on question (A, B). Assume the strategy succeeds with probability at least $1 - \varepsilon$. Recall that this includes both the test described in Figure 4.2, and the automatic consistency test. Let $C_A = \sum_{a,b}(-1)^a C^{a,b}$ and $C_B = \sum_{a,b}(-1)^b C^{a,b}$. Then C_A and C_B commute. Thus

$$\begin{aligned} A_{\mathsf{A}} B_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}} &\approx_{\sqrt{\varepsilon}} A_{\mathsf{A}} \otimes (C_B)_{\mathsf{B}} \\ &\approx_{\sqrt{\varepsilon}} \mathbb{1}_{\mathsf{A}} \otimes (C_B)_{\mathsf{B}} (C_A)_{\mathsf{B}} \\ &= \mathbb{1}_{\mathsf{A}} \otimes (C_A)_{\mathsf{B}} (C_B)_{\mathsf{B}} \\ &\approx_{\sqrt{\varepsilon}} B_{\mathsf{A}} \otimes (C_A)_{\mathsf{B}} \\ &\approx_{\sqrt{\varepsilon}} B_{\mathsf{A}} A_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}}. \end{aligned}$$

Here each approximation uses the consistency condition provided by the test, as explained in (4.1). Thus $[A, B] = (AB - BA) \approx_{\sqrt{\varepsilon}} 0$, as desired. □

We will often make use of the following simple lemma, which expresses an application of the above tests.

Lemma 18. *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and A, X observables on $\mathcal{H}_A$ such that there exists an isometry $\mathcal{H}_A \simeq \mathbb{C}^2 \otimes \mathcal{H}_{\hat{A}}$ under which the following conditions hold, for some $\delta_1, \delta_2, \delta_3$:*[6]

(i) There exists an observable A' on $\mathcal{H}_B$ such that $A \otimes \mathbb{1} \approx_{\delta_1} \mathbb{1} \otimes A'$;

(ii) $|\psi\rangle \simeq_{\delta_1} |EPR\rangle\,|AUX\rangle$ and $X \simeq_{\delta_1} \sigma_X \otimes \mathbb{1}$;

(iii) $[A, X] \approx_{\delta_2} 0$;

(iv) $\{A, X\} \approx_{\delta_3} 0$.

Then there exist Hermitian A_I, A_X, A_Y, A_Z on $\mathcal{H}_{\hat{A}}$ such that $A \simeq_{\delta_1+\delta_2} \mathbb{1} \otimes A_I + \sigma_X \otimes A_X$ and $A \simeq_{\delta_1+\delta_3} \sigma_Y \otimes A_Y + \sigma_Z \otimes A_Z$. (A similar claim holds with X replaced by Z.)

Proof. After application of the isometry, an arbitrary observable $\tilde{A}$ on $\mathbb{C}^2 \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ has a decomposition $\tilde{A} = \sum_{P \in \{I,X,Y,Z\}} \sigma_P \otimes A_P$, for Hermitian operators A_P on $\mathcal{H}_{\hat{\mathsf{A}}}$. We can compute

$$[\tilde{A}, \sigma_X \otimes \mathbb{1}] = -2i\,\sigma_Z \otimes A_Y + 2i\,\sigma_Y \otimes A_Z, \tag{4.3}$$

$$\{\tilde{A}, \sigma_X \otimes \mathbb{1}\} = 2\,\sigma_X \otimes A_I + 2\,\sigma_I \otimes A_X. \tag{4.4}$$

[6] Note that we allow either δ_i to equal 1, leading to a vacuous condition.

Assumptions (i) and (ii) imply $[A, X] \simeq_{\delta_1} [\tilde{A}, \sigma_X \otimes \mathbb{1}]$, so by (iii) and (4.3) we get $\| A_Y |\text{AUX}\rangle \|^2 + \| A_Z |\text{AUX}\rangle \|^2 = O(\delta_1 + \delta_2)$. Similarly, (iv) and (4.4) give $\| A_I |\text{AUX}\rangle \|^2 + \| A_X |\text{AUX}\rangle \|^2 = O(\delta_1 + \delta_3)$. □

4.3.2 The Bell basis

Given two commuting pairs of anti-commuting observables $\{X_1, Z_1\}$ and $\{X_2, Z_2\}$ we provide a test for a four-outcome projective measurement in the Bell basis specified by these observables, i.e. the joint eigenbasis of X_1X_2 and Z_1Z_2. The same test can be extended to test the "SW" observable,

$$\text{SW} = \frac{1}{2}\big(\mathbb{1} + X_1X_2 + Z_1Z_2 - (X_1Z_1)(X_2Z_2)\big), \tag{4.5}$$

which exchanges the qubits specified by each pair of observables. The Bell measurement test described in Figure 4.3 tests for both.

Test $\textsc{Bell}(X_1, X_2, Z_1, Z_2)$:

- Inputs: For $i \in \{1, 2\}$, $\{X_i, Z_i\}$ observables, $\{\Phi^{ab}\}_{a,b\in\{0,1\}}$ a four-outcome projective measurement, and SW an observable, all acting on the same space $\mathcal{H}$.
- Relations: for all $a, b \in \{0, 1\}$, $\Phi^{ab} = \frac{1}{4}\big(\mathbb{1} + (-1)^a Z_1Z_2\big)\big(\mathbb{1} + (-1)^b X_1X_2\big)$, and $\text{SW} = \Phi^{00} + \Phi^{01} + \Phi^{10} - \Phi^{11}$.
- Test: execute each of the following with equal probability:
  (a) Execute the Magic Square game, labeling each entry of the square from Figure 4.1 (except entry $(3, 3)$, labeled as Y_1Y_2) using the observables X_1, Z_1 and X_2, Z_2.
  (b) Send Φ to one prover and the labels (X_1X_2, Z_1Z_2, Y_1Y_2) associated with the third column of the Magic Square to the other. The first prover replies with $a, b \in \{0, 1\}$, and the second with $c, d, e \in \{\pm 1\}$. The referee checks the provers' answers for the obvious consistency conditions. For example, if the first prover reports the outcome $(0, 0)$, then the referee rejects if $(c, d) \neq (+1, +1)$.
  (c) Send Φ to one prover and SW to the other. The first prover replies with $a, b \in \{0, 1\}$, and the second with $c \in \{\pm 1\}$. Accept if and only $c = (-1)^{ab}$.

Figure 4.3: The Bell measurement test.

Lemma 19. *The test* $\textsc{Bell}(X_1, X_2, Z_1, Z_2)$ *is a robust* $(1, \delta)$ *self-test for*

$$\mathcal{R} = \Big\{ \{\Phi^{ab}\}_{a,b\in\{0,1\}} \in \text{Proj}, SW \in \text{Obs} \Big\} \cup \Big\{ \Phi^{ab} = \frac{1}{4}\big(1 + (-1)^a Z_1Z_2\big)\big(1 + (-1)^b X_1X_2\big) \Big\} \\ \cup \big\{ SW = \Phi^{00} + \Phi^{01} + \Phi^{10} - \Phi^{11} \big\},$$

for some $\delta(\varepsilon) = O(\sqrt{\varepsilon})$.

Proof. Completeness is clear: the provers can play the honest strategy for the Magic Square game, use a measurement in the Bell basis on their two qubits for Φ, and measure the observable in (4.5) for SW.

For soundness, let $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$, $\{W_1 W_2' : W, W' \in \{I, X, Z\}\}$, $\{\Phi^{ab}\}$ and SW denote a state and operators for a strategy that succeeds with probability at least $1-\varepsilon$ in the test. From the analysis of the Magic Square game (Lemma 16) it follows that the provers' observables X_1X_2 and Z_1Z_2 associated to questions with those labels approximately commute, and are each the product of two commuting observables X_1I, IX_2 and Z_1I, IZ_2 respectively, such that X_1I and Z_1I, and IX_2 and IZ_2, anti-commute; all approximate identities hold up to error $O(\sqrt{\varepsilon})$.

Since X_1X_2 and Z_1Z_2 appear together in the same question (the last column of the Magic Square, Figure 4.1), each prover has a four-outcome projective measurement $\{W^{c,d}\}_{c,d\in\{0,1\}}$ such that $\sum_d (-1)^c W^{c,d} = X_1X_2$ and $\sum_c (-1)^d W^{c,d} = Z_1Z_2$, from which it follows that $W^{c,d} = (1/4)(1 + (-1)^c Z_1Z_2)(1 + (-1)^d X_1X_2)$.

The prover's success probability in part (b) of the test is then

$$\sum_{a,b} \langle\psi| \Phi^{ab} \otimes W^{a,b} |\psi\rangle = \sum_{a,b} \langle\psi| \Phi^{ab} \otimes \frac{1}{4}\big(1 + (-1)^a Z_1Z_2\big)\big(1 + (-1)^b X_1X_2\big) |\psi\rangle .$$

Using that, by assumption, $\{\Phi^{ab}\}$ is a projective measurement, the condition that this expression be at least $1 - O(\varepsilon)$ implies

$$\Phi^{ab} \otimes \mathbb{1} \approx_{\sqrt{\varepsilon}} \mathbb{1} \otimes \frac{1}{4}\big(1 + (-1)^a Z_1Z_2\big)\big(1 + (-1)^b X_1X_2\big).$$

Combining this with the implicit consistency test yields the first relation. The last is guaranteed by part (c) of the test, which checks for the correct relationship between SW and Φ; the analysis is similar. □

4.3.3 The m-qubit Pauli group

In this section we formulate a robust self-test for the m-qubit Pauli group. The result is a slight extension of the results from [69] to allow testing of σ_Y observables.

4.3.3.1 The m-qubit Weyl-Heisenberg group

We start by giving a self-test for tensor products of σ_X and σ_Z observables acting on m qubits, i.e. the m-qubit Weyl-Heisenberg group $\mathcal{H}^{(m)}$ (see Section 4.2.2.1). Let $\mathcal{P}^{(m)}$ denote the relations

$$\begin{aligned}\mathcal{P}_d^{\otimes\{}X,Z\} = &\left\{W(a) \in \text{Obs},\, W \in \prod_{i=1}^{m}\{X_i, Z_i\},\, a \in \{0,1\}^m\right\} \\ &\cup \left\{W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W_i' \wedge a_i a_i' = 1\}|}W'(a')W(a),\, \forall a, a' \in \{0,1\}^m\right\} \\ &\cup \left\{W(a)W(a') = W(a+a'),\, \forall a, a' \in \{0,1\}^m\right\}.\end{aligned}$$

Recall the notation $W(a)$ for the string that is W_i when $a_i = 1$ and I otherwise. The first set of relations expresses the canonical anti-commutation relations. The second set of relations expresses the obvious relations $\sigma_W \mathbb{1} = \mathbb{1}\sigma_W$ and $\sigma_W^2 = \mathbb{1}$, for $W \in \{X, Z\}$, coordinate-wise. It is easy to verify that $\mathcal{P}^{(m)}$ forms a defining set of relations for $\mathcal{H}^{(m)}$. Our choice of relations is suggested by the Pauli Braiding test introduced in [69], which shows that the relations are testable with a robustness parameter $\delta(\varepsilon)$ that is independent of m. The underlying test is called the Pauli Braiding test, and denoted $\textsc{pbt}(X, Z)$. For convenience here we use a slight variant of the test, which includes more questions; the test is summarized in Figure 4.4.

Test $\textsc{pbt}(X, Z)$:

- Inputs: (W, a), for $W \in \prod_{i=1}^{n}\{X_i, Z_i\}$ and $a \in \{0,1\}^m$.
- Relations: $\mathcal{P}_d^{\otimes\{}X, Z\}$.
- Test: Perform the following with probability $1/2$ each:
  (a) Select $W, W' \in \prod_i \{X_i, Z_i\}$, and $a, a' \in \{0,1\}^m$, uniformly at random. If $\{i : W_i \neq W_i' \wedge a_i = a_i' = 1\}$ has even cardinality then execute test $\textsc{com}(W(a), W'(a'))$. Otherwise, execute test $\textsc{ac}(W(a), W'(a'))$.
  (b) Select $(a, a') \in \{0,1\}^m$ and $W \in \prod_{i=1}^{m}\{X_i, Z_i\}$ uniformly at random. Execute test $\textsc{prod}(W(a), W(a'), W(a+a'))$.

Figure 4.4: The Pauli Braiding test, $\textsc{pbt}(X, Z)$.

The following lemma follows immediately from the definition of the relations $\mathcal{P}_d^{\otimes\{}X, Z\}$ and the analysis of the tests COM, PROD and AC given in Section 4.3.1.

Lemma 20 (Theorem 13 [69])**.** *The test $\textsc{pbt}(X, Z)$ is a robust $(1, \delta)$ self-test for $\mathcal{P}_d^{\otimes\{}X, Z\}$, for some $\delta(\varepsilon) = O(\varepsilon^{1/2})$.*

In addition we need the following lemma, which states that observables approximately satisfying the relations $\mathcal{P}_d^{\otimes\{}X, Z\}$ are close to operators which, up to a local isometry, behave exactly as a tensor product of Pauli σ_X and σ_Z observables.

Lemma 21 (Theorem 14 [69])**.** *The set of relations $\mathcal{P}^{(n)}$ is δ-stable, with $\delta(\varepsilon) = O(\varepsilon)$.*

Lemma 21 is proved in [69] with a polynomial dependence of δ on ε. The linear dependence can be established by adapting the results of [98] to the present setting; we omit the details (see [97]).

The following lemma is an extension of Lemma 18 to the case of multi-qubit Pauli observables; the lemma avoids any dependence of the error on the number of qubits, as would follow from a sequential application of Lemma 18.

Lemma 22. *Let n be an integer, $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and A and $X(a)$, for $a \in \{0,1\}^m$, observables on $\mathcal{H}_A$ such that there exists an isometry $\mathcal{H}_A \simeq (\mathbb{C}^2)^{\otimes m} \otimes \mathcal{H}_{\hat{A}}$ under which the following conditions hold, for some $\delta_1, \delta_2, \delta_3$:*

(i) There exists an observable A' on $\mathcal{H}_B$ such that $A \otimes \mathbb{1} \approx_{\delta_1} \mathbb{1} \otimes A'$;

(ii) $|\psi\rangle \simeq_{\delta_1} |EPR\rangle^{\otimes m} |AUX\rangle$, and $X(a) \simeq_{\delta_1} \sigma_X(a) \otimes \mathbb{1}$;

(iii) $[A, X(a)] \simeq_{\delta_2} 0$;

(iv) For some $c \in \{0,1\}^m$ and $a \cdot c = 1$, $\{A, X(a)\} \simeq_{\delta_3} 0$,

where the first two conditions are meant on average over a uniformly random $a \in \{0,1\}^m$, and the last over a uniformly random a such that $a \cdot c = 1$. For $P \in \{I, X, Y, Z\}^m$ let $x_P \in \{0,1\}^m$ be such that $(x_P)_i = 1$ if and only if $P_i \in \{Y, Z\}$. Then there exists Hermitian A_P, for $P \in \{I, X, Y, Z\}^m$, on $\mathcal{H}_{\hat{A}}$ such that

$$A \simeq_{\delta_1+\delta_2} \sum_{P \in \{I,X\}^n} \sigma_P \otimes A_P\,, \qquad \text{and} \qquad A \simeq_{\delta_1+\delta_3} \sum_{\substack{P \in \{I,X,Y,Z\}^m: \\ c_i=1 \Rightarrow P_i \in \{Y,Z\} \\ c_i=0 \Rightarrow P_i \in \{I,X\}}} \sigma_P \otimes A_P\,.$$

(A similar claim holds with X replaced by Z.)

Proof. After application of the isometry, an arbitrary observable $\tilde{A}$ on $(\mathbb{C}^2)^{\otimes m} \otimes \mathcal{H}_{\hat{A}}$ has a decomposition $\tilde{A} = \sum_{P \in \{I,X,Y,Z\}^m} \sigma_P \otimes A_P$, for Hermitian operators A_P on $\mathcal{H}_{\hat{A}}$. Then the analogue of (4.3) is

$$[\tilde{A}, \sigma_X(a) \otimes \mathbb{1}] = 2 \sum_{P:\, a \cdot x_P = 1} \sigma_P \sigma_X(a) \otimes A_P\,.$$

Using that any string x_P which is not the 0^m string satisfies $a \cdot x_P = 1$ with probability almost $1/2$ for a uniform choice of a, orthogonality of the $\sigma_P \sigma_X(a)$ for distinct P lets us conclude the proof of the first relation as in Lemma 18. Similarly, the analogue of (4.4) gives

$$\{\tilde{A}, \sigma_X(a) \otimes \mathbb{1}\} = 2 \sum_{P:\, a \cdot x_P = 0} \sigma_P \sigma_X(a) \otimes A_P \,.$$

Using that any string x_P which is not c satisfies $a \cdot x_P = 0$ with probability almost $1/2$ for a uniform choice of a such that $a \cdot c = 1$, orthogonality of the $\sigma_P \sigma_X(a)$ for distinct P lets us conclude the proof of the second relation. □

4.3.3.2 The m-qubit Pauli group

We will use an extended version of the Pauli Braiding test introduced in Section 4.3.3.1 which allows to test for a third observable, Y_i, on each system. Ideally we would like to enforce the relation $Y_i = \sqrt{-1} X_i Z_i$. Unfortunately, the complex phase cannot be tested from classical correlations alone: complex conjugation leaves correlations invariant, but does not correspond to a unitary change of basis (see [82, Appendix A] for a discussion of this issue).

We represent the "choice" of complex phase, $\sqrt{-1}$ or its conjugate $-\sqrt{-1}$, by an observable Δ that the prover measures on a system that is in a tensor product with all other systems on which the prover acts. Informally, the outcome obtained when measuring Δ tells the prover to use $Y = iXZ$ or $Y = -iXZ$.

We first introduce Y and test that the triple $\{X, Y, Z\}$ pairwise anticommute at each site. This corresponds to the following set of relations:

$$\begin{aligned}
\mathcal{P}^{(m)}\{X, Y, Z\} = &\left\{ W(a) \in \text{Obs},\, W \in \{X, Y, Z\}^n,\, a \in \{0,1\}^n \right\} \\
&\cup \left\{ W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W'_i \wedge a_i a'_i = 1\}|} W'(a')W(a),\, \forall a, a' \in \{0,1\}^n \right\} \\
&\cup \left\{ W(a)W(a') = W(a + a'),\, \forall a, a' \in \{0,1\}^n \right\}.
\end{aligned}$$

Test $\textsc{pbt}(X, Y, Z)$:

- Inputs: $W \in \prod_{i=1}^{m} \{X, Y, Z\}$
- Relations: $\mathcal{P}_d^{\otimes\{}X, Y, Z\}$.
- Test: Perform the following with equal probability:
  (a) Execute test $\textsc{pbt}(X^m, Z^m)$.
  (b) Execute test $\textsc{pbt}(Y^m, X^m)$ or test $\textsc{pbt}(Y^m, Z^m)$, chosen with probability $1/2$ each.
  (c) Select a random permutation $\sigma \in \mathfrak{S}_{m/2}$, and $W \in \{I, Y\}^m$ uniformly at random. Write $W = W_1 W_2$, where $W_1, W_2 \in \{I, Y\}^{m/2}$. Let W_1^σ be the string W_1 with its entries permuted according to σ. Do the following with equal probability:
    (i) Send one prover $W_1 W_1^\sigma$ and the other either $W_1 W_2$ or $W_2 W_1^\sigma$ (chosen with probability $1/2$), and check consistency of the first or second half of the provers' answer bits.
    (ii) Send one prover $W_1 W_1^\sigma$, and the other $\prod_i \Phi_{i,\sigma(i)}$, where each $\Phi_{i,\sigma(i)}$ designates a measurement in the Bell basis for the $(i, m/2 + \sigma(i))$ pair of qubits. The first prover replies with $a \in \{\pm 1\}^m$, and the second with $b \in \{00, 01, 10, 11\}^{m/2}$. For each $i \in \{1, \ldots, m/2\}$ such that $b_i = 00$, check that $a_i = a_{m/2+\sigma(i)}$.
    (iii) Execute $m/2$ copies of test $\textsc{Bell}$ (in parallel), for qubit pairs $(i, m/2 + \sigma(i))$, for $i \in \{1, \ldots, m/2\}$.

Figure 4.5: The extended Pauli Braiding test, $\textsc{pbt}(X, Y, Z)$.

The test is described in Figure 4.5. It has three components. Part (a) of the test executes $\textsc{pbt}(X^m, Z^m)$, which gives us multi-qubit Pauli X and Z observales. Part (b) of the test introduces observables labeled $Y(c)$, and uses tests $\textsc{pbt}(Y^m, X^m)$ and $\textsc{pbt}(Y^m, Z^m)$ to enforce appropriate anti-commutation relations with the Pauli X and Z observables obtained in part (a). Using Lemma 22, this part of the test will establish that the $Y(c)$ observables approximately respect the same n-qubit tensor product structure as $X(a)$ and $Z(b)$.

Part (c) of the test is meant to control the "phase" ambiguity in the definition of $Y(c)$ that remains after the analysis of part (b). Indeed, from that part it will follow that $Y(c) \simeq \sigma_Y(c) \otimes \Delta(c)$, where $\Delta(c)$ is an arbitrary observable acting on the ancilla system produced by the isometry obtained in part (a). We would like to impose $\Delta(c) \approx \Delta_Y^{|c|}$ for a fixed observable Δ_Y which represents the irreducible phase degree of freedom in the definition of Y, as discussed above. To obtain this, part (c) of the test performs a form of SWAP test between different $Y(c)$ observables, enforcing that e.g. $Y(1, 0, 1)$ is consistent with $Y(0, 1, 1)$ after an appropriate Bell measurement has "connected" registers 1 and 2. The swapping is defined using Pauli σ_X and σ_Z, which leave the ancilla register

invariant; consistency will then imply $\Delta(1,0,1) \approx \Delta(0,1,1)$.

Lemma 24 (restated). *Suppose $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_A)$, for $W \in \{X,Y,Z\}^m$ and $a \in \{0,1\}^m$, specify a strategy for the players that has success probability at least $1-\varepsilon$ in the extended Pauli Braiding test $\textsc{pbt}(X,Y,Z)$ described in Figure 4.5. Then there exist isometries $V_D : \mathcal{H}_D \to ((\mathbb{C}^2)^{\otimes m})_{D'} \otimes \hat{\mathcal{H}}_{\hat{D}}$, for $D \in \{A,B\}$, such that*

$$\left\| (V_A \otimes V_B) \, |\psi\rangle_{AB} - |EPR\rangle_{A'B'}^{\otimes n} \, |\textsc{aux}\rangle_{\hat{A}\hat{B}} \right\|^2 = O(\sqrt{\varepsilon}),$$

and on expectation over $W \in \{X,Y,Z\}^m$,

$$\mathbb{E}_{a\in\{0,1\}^m} \left\| \left(W(a) - V_A^\dagger(\sigma_W(a) \otimes \Lambda_W(a)) V_A\right) \otimes \mathbb{1}_B \, |\psi\rangle \right\|^2 = O(\sqrt{\varepsilon}),$$

where $\Lambda_W(a) = \prod_i \Lambda_{W_i}^{a_i} \in \mathrm{Obs}(\mathcal{H}_{\hat{A}})$ are observables with $\Delta_X = \Delta_Z = \mathbb{1}$ and Δ_Y an arbitrary observable on $\hat{\mathcal{H}}$ such that

$$\left\| \Delta_Y \otimes \Delta_Y \, |\textsc{aux}\rangle - |\textsc{aux}\rangle \right\|^2 = O(\sqrt{\varepsilon}).$$

Proof sketch. The existence of the isometries V_A and V_B follows from part (a) of the test and the combination of Lemma 20 and Lemma 21; see e.g. [69] for an explicit construction. Under this isometry we have $X(a) \simeq_{\sqrt{\varepsilon}} \sigma_X(a)$ and $Z(b) \simeq_{\sqrt{\varepsilon}} \sigma_Z(b)$, on average over $a,b \in \{0,1\}^m$. Applying the second part of Lemma 22, the anti-commutation relations between $Y(c)$ and $X(a)$ and $Z(b)$ verified in part (b) of the test imply that under the same isometry,

$$Y(c) \simeq \sigma_Y(c) \otimes \Delta(c),$$

for some observable $\Delta(c)$ on $\mathcal{H}_{\hat{A}}$. Using the linearity relations that are verified in the $\textsc{pbt}$ test, we may in addition express $\Delta(c) = \prod_i \Delta_i^{c_i}$ for (perfectly) commuting observables Δ_i. Using Claim 1 below, success at least $1 - O(\varepsilon)$ in part (c) of the test then implies that on average over a random permutation $\sigma \in \mathcal{S}_{n/2}$,

$$\mathbb{E}_\sigma \, \mathbb{E}_{c\in\{0,1\}^{m/2}} \, 2^{-m} \, \mathrm{Tr}\left(\sigma_Y(c,c^\sigma)\right) \, \langle \textsc{aux}| \left(\prod_{i=1}^{m/2} \left(\Delta_i \Delta_{m/2+\sigma(i)}\right)^{c_i} \right) |\textsc{aux}\rangle = 1 - O(\sqrt{\varepsilon}), \quad (4.6)$$

where we wrote (c,c^σ) for the m-bit string $(c_1,\ldots,c_{m/2},c_{\sigma(1)},\ldots,c_{\sigma(m/2)})$. Defining

$$\Delta_Y \;=\; \mathbb{E}_{i\in\{\frac{m}{2}+1,\ldots,m\}} \frac{\Delta_i}{|\mathbb{E}_i \Delta_i|}, \quad (4.7)$$

Eq. (4.6) readily implies that $\Delta(c) \approx_{\sqrt{\varepsilon}} \Delta_Y^{|c|}$. In slightly more detail, we first observe that

$$\begin{aligned} &\mathbb{E}_{c\in\{0,1\}^{m/2}} \left\| \left(\Delta(c) - \left(\mathbb{E}_{i\in\{\frac{m}{2}+1,\ldots,m\}} \Delta_i\right)^{|c|} \right) |\textsc{aux}\rangle \right\|^2 \\ &\leq \mathbb{E}_c \mathbb{E}_{g:\{1,\ldots,\frac{m}{2}\}\to\{\frac{m}{2}+1,\ldots,m\}} \left\| \left(\Delta(c) - \prod_i \Delta_{g(i)}^{c_i} \right) |\textsc{aux}\rangle \right\|^2. \end{aligned} \quad (4.8)$$

where the first inequality is by convexity, with the expectation taken over a random function g. We would like to relate this last term to the expectation over a random permutation $\sigma \in \mathcal{S}_{m/2}$. One way to do this is to observe that with probability $1 - O(1/m)$ over the choice of a uniformly random g it is possible to write

$$\prod_i \Delta_{g(i)}^{c_i} = \Big(\prod_i \Delta_{m/2+\tau'(i)}^{c'_i}\Big)\Big(\prod_i \Delta_{m/2+\tau''(i)}^{c''_i}\Big),$$

where $c'_i + c''_i = c_i$ for all i, τ', τ'' are permutations such that $m/2 + \tau'(i) = g(i)$ if $c'_i = c_i$, and $m/2 + \tau''(i) = g(i)$ if $c''_i = c_i$; this is possible because g might have two-element collisions, but is unlikely to have any three-element collisions. Moreover, for uniformly random c and g we can ensure that the marginal distribution on (c', τ') and (c', τ'') is uniform. This allows us to use (4.6) twice to bound the right-hand side of (4.8) by $O(\sqrt{\varepsilon})$ (after having expanded the square). As a consequence, $\mathbb{E}_i \Delta_i$ is close to an observable, and it is then routine to show that Δ_Y defined in (4.7) satisfies $\Delta(c) \approx_{\sqrt{\varepsilon}} \Delta_Y^{|c|}$, on average over a uniformly random c.

The last condition in the lemma follows from the consistency relations, which imply that $X(a) \otimes X(a)$, $Z(b) \otimes Z(b)$ and $Y(c) \otimes Y(c)$ all approximately stabilize $|\psi\rangle$; then $\Delta_Y^{|a|} \otimes \Delta_Y^{|a|} \approx X(a)Z(a)Y(a) \otimes X(a)Z(a)Y(a)$ also does. □

Claim 1. *Let $A \in \mathrm{Obs}(\mathbb{C}^2_{A_1} \otimes \cdots \otimes \mathbb{C}^2_{A_k} \otimes \mathcal{H})$ and $B \in \mathrm{Obs}(\mathbb{C}^2_{B_1} \otimes \cdots \otimes \mathbb{C}^2_{B_k} \otimes \mathcal{H})$ be k-qubit observables acting on distinct registers A_j, B_j, as well as a common space $\mathcal{H}$, and $\Phi_{\mathsf{A'B'}} = \prod_{j=1}^k |EPR\rangle\langle EPR|_{\mathsf{A'}_j,\mathsf{B'}_j}$ the the projector on k EPR pairs across registers $\mathsf{A'}_j$ and $\mathsf{B'}_j$. Then*

$$\Big(\bigotimes_j \langle EPR|_{\mathsf{A}_j\mathsf{A'}_j} \langle EPR|_{\mathsf{B}_j\mathsf{B'}_j} \otimes \mathbb{1}_{\mathcal{H}}\Big)\Big((A_{\mathsf{A}\mathcal{H}} \otimes \mathbb{1}_{\mathsf{B}})(\mathbb{1}_{\mathsf{A}} \otimes B_{\mathsf{B}\mathcal{H}}) \otimes \Phi_{\mathsf{A'B'}}\Big)\Big(\bigotimes_j |EPR\rangle_{\mathsf{A}_j\mathsf{A'}_j} |EPR\rangle_{\mathsf{B}_j\mathsf{B'}_j} \otimes \mathbb{1}_{\mathcal{H}}\Big)$$
$$= \frac{1}{2^{2k}} \sum_i \mathrm{Tr}\left(A_i B_i\right) A'_i B'_i, \tag{4.9}$$

where we write $A = \sum_i A_i \otimes A'_i$ and $B = \sum_i B_i \otimes B'_i$, for A_i on $\mathcal{H}_{\mathsf{A}}$, B_i on $\mathcal{H}_{\mathsf{B}}$, and A'_i, B'_i on $\mathcal{H}$.

Proof. We do the proof for $k = 1$, as the general case is similar. Using that for any operators X_{AB} and $Y_{\mathsf{A'B'}}$,

$$\langle \mathrm{EPR}|_{\mathsf{AA'}} \langle \mathrm{EPR}|_{\mathsf{BB'}} \left(X_{\mathsf{AB}} \otimes Y_{\mathsf{A'B'}}\right) |\mathrm{EPR}\rangle_{\mathsf{AA'}} |\mathrm{EPR}\rangle_{\mathsf{BB'}} = \frac{1}{4} \mathrm{Tr}\Big(XY^T\Big),$$

the left-hand side of (4.9) evaluates to

$$4^{-1} \mathrm{Tr}_{\mathsf{AB}}\left((A_{\mathsf{A}\mathcal{H}} \otimes \mathbb{1}_{\mathsf{B}})(\mathbb{1}_{\mathsf{A}} \otimes B_{\mathsf{B}\mathcal{H}})(\Phi^T_{\mathsf{A'B'}} \otimes \mathbb{1}_{\mathcal{H}})\right),$$

which using the same identity again gives the right-hand side of (4.9). □

4.4 Testing products of Clifford observables

This subsection contains our main original extension of the Pauli Braiding test to certify the measurement of any product of single-qubit Clifford observable on many EPR pairs.

In Section 4.4.1, we give a test for the conjugation of one observable to another by a unitary, the Conjugation Test. In Section 4.4.2, we will apply the Conjugation Test to test the relations that dictate how an arbitrary m-qubit Clifford unitary acts by conjugation on the Pauli matrices. In Section 4.4.3 we specialize the test to the case of unitaries that can be expressed as the m-fold tensor product of Clifford observables taken from the set Σ. In Sections 4.4.4 and 4.4.5, we decribe variants of the test from Section 4.4.3, which are later employed in the Leash and Dog-Walker protocols.

4.4.1 The conjugation test

We give a test which certifies that a unitary (not necessarily an observable) conjugates one observable to another. More precisely, let A, B be observables, and R a unitary, acting on the same space $\mathcal{H}$. The test $\textsc{conj}(A, B, R)$, given in Figure 4.6, certifies that the players implement observables of the form

$$X_R = \begin{pmatrix} 0 & R^\dagger \\ R & 0 \end{pmatrix} \qquad \text{and} \qquad C = C_{A,B} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \tag{4.10}$$

such that X_R and C commute. The fact that X_R is an observable implies that R is unitary,[7] while the commutation condition is equivalent to the relation $RAR^\dagger = B$. The test thus tests for the relations

$$\mathcal{C}\{R, C\} = \{X_R, C, X, Z \in \text{Obs}\} \cup \{XZ = -ZX\} \cup \{X_R C = CX_R,\ X_R Z = -ZX_R,\ CZ = ZC\}.$$

Here the anti-commuting observables X and Z are used to specify a basis in which X_R and C can be block-diagonalized. The anti-commutation and commutation relations with Z enforce that X_R and C respectively have the form described in (4.10). These relations are enforced using simple commutation and anti-commutation tests that are standard in the literature on self-testing. For convenience, we state those tests, COM and AC, in Appendix 4.2.2. The conjugation test, which uses them as sub-tests, is given in Figure 4.6. Here, "Inputs" refers to a subset of designated questions in the test; "Relation" indicates a relation that the test aims to certify; "Test" describes the certification protocol. (Recall that all our protocols implicitly include a "consistency" test in which a question is chosen uniformly at random from the marginal distribution and sent to both players, whose answers are accepted if and only if they are equal.)

[7] Note that R will not be directly accessed in the test, since by itself it does not necessarily correspond to a measurement.

Test CONJ(A,B,R)

- Inputs: A and B observables on the same space $\mathcal{H}$, and X and Z observables on $\mathcal{H}'$. X_R and C observables on $\mathcal{H} \otimes \mathcal{H}'$.
- Relations: $\mathcal{C}\{R, C\}$, with R defined from X_R, and C related to A and B, as in (4.10).
- Test: execute each of the following with equal probability
  (a) With probability $1/8$ each, execute tests $\text{AC}(X, Z)$, $\text{COM}(C, Z)$, $\text{COM}(X_R, C)$, $\text{AC}(X_R, Z)$ and $\text{COM}(A, X)$, $\text{COM}(B, X)$, $\text{COM}(A, Z)$, $\text{COM}(B, Z)$.
  (b) Ask one player to measure A, B, C or Z (with probability $1/4$ each), and the other to jointly measure A or B (with probability $1/2$ each) and Z. The first player returns one bit, and the second two bits. Reject if either:
    – The first player was asked C, the second player was asked (A, Z), his second answer bit is 0, and his first answer bit does not match the first player's;
    – The first player was asked C, the second player was asked (B, Z), his second answer bit is 1, and his first answer bit does not match the first player's.
    – The first player was asked A, B, or Z and his answer bit does not match the corresponding answer from the second player.

Figure 4.6: The conjugation test, $\text{CONJ}(A, B, R)$.

Lemma 23. *The test* $\text{CONJ}(A, B, R)$ *is a* $(1, \delta)$ *self-test for the set of relations* $\mathcal{C}\{R, C\}$*, for some* $\delta = O(\sqrt{\varepsilon})$*. Moreover, for any strategy that succeeds with probability at least* $1 - \varepsilon$ *in the test it holds that* $C \approx_\delta A(\mathbb{1} + Z)/2 + B(\mathbb{1} - Z)/2$*, where* A, B, C *and* Z *are the observables applied by the prover on receipt of a question with the same label.*

Proof. Completeness is clear, as players making measurements on a maximally entangled state on $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$, tensored with an EPR pair on $\mathbb{C}^2 \otimes \mathbb{C}^2$ for the X and Z observables, and using X_R and C defined in (4.10) (with the blocks specified by the space associated with each player's half-EPR pair) succeed in each test with probability 1.

We now consider soundness. Success in $\text{AC}(X, Z)$ in part (a) of the test implies the existence of local isometries V_A, V_B such that $V_A : \mathcal{H}_\mathsf{A} \to \mathcal{H}_{\hat{\mathsf{A}}} \otimes \mathbb{C}^2_{\mathsf{A}'}$, with $X \simeq_{\sqrt{\varepsilon}} \mathbb{1}_{\hat{\mathsf{A}}} \otimes \sigma_X$ and $Z \simeq_{\sqrt{\varepsilon}} \mathbb{1}_{\hat{\mathsf{A}}} \otimes \sigma_Z$. By Lemma 18, approximate commutation with both X and Z implies that under the same isometry, $A \simeq_{\sqrt{\varepsilon}} A_I \otimes \mathbb{1}$ and $B \simeq_{\sqrt{\varepsilon}} B_I \otimes \mathbb{1}$, for observables A_I, B_I on $\mathcal{H}_{\hat{\mathsf{A}}}$. Similarly, the parts of the test involving C and X_R imply that they each have the block decomposition specified in (4.10). In particular, anti-commutation of X_R with Z certifies that X_R has a decomposition of the form $X_R \simeq R_X \otimes \sigma_X + R_Y \otimes \sigma_Y$. Using that X_R is an observable, we deduce that there exists a

unitary R on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that $R \approx R_X + iR_Y$. Similarly, commutation of C with Z implies that $C \simeq C_I \otimes I + C_Z \otimes \sigma_Z$, for Hermitian C_I, C_Z such that $C_I \pm C_Z$ are observables.

Next we analyze part (b) of the test. Let $\{W_{AZ}^{a,z}\}$ be the projective measurement applied by the second player upon query (A, Z). Success with probability $1 - O(\varepsilon)$ in the first item ensures that

$$\left| \langle\psi| C \otimes (W_{AZ}^{00} - W_{AZ}^{10}) |\psi\rangle \right| = O(\varepsilon),$$

and a similar condition holds from the second item, with W_{BZ} instead of W_{AZ}. Success with probability $1 - O(\varepsilon)$ in the third item ensures consistency of $\{W_{AZ}^{a,z}\}$ (resp. $\{W_{BZ}^{a,z}\}$) with the observable A (resp. B) when marginalizing over the second outcome, and Z when marginalizing over the first outcome. Using the decompositions for A, B and C derived earlier, we obtain $C_I \approx (A + B)/2$ and $C_Z \approx (A - B)/2$, giving the "Moreover" part of the lemma.

Finally, success in test $\textsc{com}(X_R, C)$ certifies the approximate commutation relation $[X_R, C] \approx_{\sqrt{\varepsilon}} 0$, which, given the decomposition of X_R and C obtained so far, implies $RA \approx BR$, as desired. □

4.4.2 Testing Clifford unitaries

Let $m \geq 1$ be an integer, and R an m-qubit Clifford unitary. R is characterized, up to phase, by its action by conjugation on the m-qubit Weyl-Heisenberg group. This action is described by linear functions $h_S : \{0,1\}^m \times \{0,1\}^m \to \mathbb{Z}_4$ and $h_X, h_Z : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}^m$ such that

$$R\sigma_X(a)\sigma_Z(b)R^\dagger = (-1)^{h_S(a,b)}\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)), \qquad \forall a, b \in \{0,1\}^m. \tag{4.11}$$

Using that $(\sigma_X(a)\sigma_Z(b))^\dagger = (-1)^{a\cdot b}\sigma_X(a)\sigma_Z(b)$, the same condition must hold of the right-hand side of (4.11), thus $h_X(a,b) \cdot h_Z(a,b) = a \cdot b \mod 2$. To any family of observables $\{X(a), Z(b),\ a, b \in \{0,1\}^m\}$ we associate, for $a, b \in \{0,1\}^m$,

$$A(a,b) = i^{a\cdot b}X(a)Z(b), \qquad B(a,b) = i^{a\cdot b}X(h_X(a,b))Z(h_Z(a,b)), \tag{4.12}$$

where the phase $i^{a\cdot b}$ is introduced to ensure that $A(a,b)$ and $B(a,b)$ are observables. Define $C(a,b)$ in terms of $A(a,b)$ and $B(a,b)$ as in (4.10). The Clifford conjugation test aims to test for the conjugation relation $RA(a,b)R^\dagger = B(a,b)$, for all (in fact, on average over a randomly chosen) (a,b). For this, we first need a test that ensures $A(a,b)$ and $B(a,b)$ themselves have the correct form, in terms of a tensor product of Pauli observables. Such a test was introduced in [69], where it is called "Pauli Braiding test". The test certifies the Pauli relations

$$\begin{aligned}\mathcal{P}^{(m)}\{X,Y,Z\} = &\Big\{W(a) \in \text{Obs},\ W \in \{X,Y,Z\}^m,\ a \in \{0,1\}^m\Big\} \\ &\cup \Big\{W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W'_i \wedge a_i a'_i = 1\}|}W'(a')W(a),\ \forall W, W' \in \{X,Y,Z\}^n,\ \forall a, a' \in \{0,1\}^m\Big\} \\ &\cup \Big\{W(a)W(a') = W(a+a'),\ \forall a, a' \in \{0,1\}^m\Big\}.\end{aligned}$$

The Pauli Braiding test is recalled in Appendix 4.3.3, and we refer to the test as $\textsc{pbt}(X,Y,Z)$. The original test from [69] only allows to test for tensor products of σ_X and σ_Z Pauli observables, and we extend the test to include Pauli σ_Y. This requires us to provide a means to accommodate the phase ambiguity discussed earlier. The result is described in the following lemma; we refer to Appendix 4.3.3.2 for the proof. (In some cases a simpler variant of the test, which does not attempt to test for the Y observable, will suffice. This is essentially the original test from [69], which we call $\textsc{pbt}(X,Z)$ and is introduced in Appendix 4.3.3.1.)

Lemma 24. *Suppose $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_A)$, for $W \in \{X,Y,Z\}^m$ and $a \in \{0,1\}^m$, specify a strategy for the players that has success probability at least $1-\varepsilon$ in the extended Pauli Braiding test $\textsc{pbt}(X,Y,Z)$ described in Figure 4.5. Then there exist a state $|\textsc{aux}\rangle_{\hat{A}\hat{B}}$ and isometries $V_D : \mathcal{H}_D \to ((\mathbb{C}^2)^{\otimes m})_{D'} \otimes \hat{\mathcal{H}}_{\hat{D}}$, for $D \in \{A,B\}$, such that*

$$\left\| (V_A \otimes V_B)\,|\psi\rangle_{AB} - |EPR\rangle^{\otimes m}_{A'B'}\,|\textsc{aux}\rangle_{\hat{A}\hat{B}} \right\|^2 = O(\sqrt{\varepsilon}),$$

and on expectation over $W \in \{X,Y,Z\}^m$,

$$\mathbb{E}_{a\in\{0,1\}^m} \left\| \left(W(a) - V_A^\dagger(\sigma_W(a)\otimes \Delta_W(a))V_A\right) \otimes \mathbb{1}_B\,|\psi\rangle \right\|^2 = O(\sqrt{\varepsilon}),$$

where $\Delta_W(a) = \prod_i \Delta_{W_i}^{a_i} \in \mathrm{Obs}(\mathcal{H}_{\hat{A}})$ are observables with $\Delta_X = \Delta_Z = \mathbb{1}$ and Δ_Y an arbitrary observable on $\hat{\mathcal{H}}$ such that

$$\left\| \Delta_Y \otimes \Delta_Y\,|\textsc{aux}\rangle - |\textsc{aux}\rangle \right\|^2 = O(\sqrt{\varepsilon}).$$

Building on the Pauli Braiding test and the conjugation test from the previous section, the Clifford conjugation test $\textsc{conj-cliff}(R)$ described in Figure 4.7 provides a test for the set of relations

$$\begin{aligned}\mathcal{J}_{h_S,h_X,h_Z}\{R\} = \mathcal{P}_d^{\otimes}\{X,Y,Z\} &\cup \{R \in \mathrm{U}\} \cup \{\Delta_Y \in \mathrm{Obs}\} \\ &\cup \left\{RX(a)Z(b)R^\dagger = \Delta_Y^{h_S(a,b)} X(h_X(a,b))Z(h_Z(a,b)),\ \forall a,b \in \{0,1\}^m\right\} \\ &\cup \left\{\Delta_Y X(a) = X(a)\Delta_Y,\ \Delta_Y Z(b) = Z(b)\Delta_Y,\ \forall a,b \in \{0,1\}^m\right\}. \qquad (4.13)\end{aligned}$$

Note the presence of the observable Δ_Y, which arises from the conjugation ambiguity in the definition of Y (see Lemma 24).

Test CONJ-CLIFF(R):

- Input: R an m-qubit Clifford unitary. Let h_S, h_X, h_Z be such that (4.11) holds, and $A(a,b), B(a,b)$ the observables defined in (4.12).
- Relations: $\mathcal{J}_{h_S,h_X,h_Z}\{R\}$ defined in (4.13).
- Test: execute each of the following with equal probability
  (a) Execute test PBT(X,Y,Z) on $(m+1)$ qubits, where the last qubit is called the "control" qubit;
  (b) Select $a,b \in \{0,1\}^m$ uniformly at random. Let $C(a,b)$ be the observable defined from $A(a,b)$ and $B(a,b)$ in (4.10), with the block structure specified by the control qubit. Execute test CONJ$\{A(a,b), B(a,b), R\}$. In the test, to specify query $A(a,b)$ or $B(a,b)$, represent each as a string in $\{I,X,Y,Z\}^m$ and use the same label as for the same query when it is used in part (a).

Figure 4.7: The Clifford conjugation test, CONJ-CLIFF(R).

Lemma 25. *Let R be an m-qubit Clifford unitary and h_S, h_X, h_Z such that* (4.11) *holds. Suppose a strategy for the players succeeds with probability at least $1-\varepsilon$ in test* CONJ-CLIFF(R). *Let $V_A : \mathcal{H}_A \to ((\mathbb{C}^2)^{\otimes(m+1)})_{A'} \otimes \mathcal{H}_{\hat{A}}$ be the isometry whose existence follows from part (a) of the test, and Δ_Y the observable on $\mathcal{H}_{\hat{A}'}$ that represents the phase ambiguity (see Lemma 24). Then there exists a unitary Λ_R on $\mathcal{H}_{\hat{A}}$, commuting with Δ_Y, such that*

$$\big\| \Lambda_R \otimes \Lambda_R \, |\mathrm{AUX}\rangle - |\mathrm{AUX}\rangle \, \big\|^2 = O(\mathrm{poly}(\varepsilon)). \tag{4.14}$$

Moreover, let $\hat{\tau}_R$ be any m-qubit Clifford unitary, acting on the space $(\mathbb{C}^2)^{\otimes m}$ into which the isometry V_A maps, which satisfies the relations specified in (4.13)*, where for any location $i \in \{1,\ldots,m\}$ such that $a_i = b_i = 1$ we replace $\sigma_X\sigma_Z$ by $\tau_Y = \sigma_Y \otimes (i\Delta_Y)$. Then, letting $\tau_R = \hat{\tau}_R(\mathbb{1}_{A'} \otimes \Lambda_R)$ we have that under the same isometry,*

$$R \simeq_{\mathrm{poly}(\varepsilon)} \tau_R.$$

Note that $\hat{\tau}_R$ is only defined up to phase in the lemma. Any representative will do, as the phase ambiguity can be absorbed in Λ_R. As an example, in this notation we have

$$\hat{\tau}_F = \frac{1}{\sqrt{2}}\big(-\sigma_X + \sigma_Y \otimes \Delta_Y\big), \qquad \hat{\tau}_G = \frac{1}{\sqrt{2}}\big(\sigma_X + \sigma_Y \otimes \Delta_Y\big),$$

where the "honest" single-qubit Clifford observables σ_F and σ_G are defined in (4.2).

Completeness of the test is clear, as players making measurements on $(m+1)$ shared EPR pairs using standard Pauli observables, R, and $C(a,b)$ defined in (4.10) with $A(a,b)$ and $B(a,b)$ as in (4.12) will pass all tests with probability 1.

Proof sketch. For $D \in \{A, B\}$ let V_D be the isometries that follow from part (a) of the test and Lemma 24. According to (4.12), $A(a,b)$ and $B(a,b)$ can each be expressed (up to phase) as a tensor product of X, Y, Z operators, where the number of occurrences of Y modulo 2 is $a \cdot b$ for $A(a,b)$ and $h_X(a,b) \cdot h_Z(a,b) = a \cdot b \mod 2$ for $B(a,b)$. Thus the labels used to specify the observables in $A(a,b)$ and $B(a,b)$ in part (b), together with the analysis of part (a) and Lemma 24, imply that

$$A(a,b) \simeq_{\sqrt{\varepsilon}} \sigma_X(a)\sigma_Z(b) \otimes (i\Delta_Y)^{a\cdot b} \text{ and } B(a,b) \simeq_{\sqrt{\varepsilon}} \sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes (i\Delta_Y)^{a\cdot b + h_S(a,b)},$$

under the same isometry. Applying the analysis of the conjugation test given in Lemma 23 shows that X_R must have the form in (4.10), for some R that approximately conjugates $A(a,b)$ to $B(a,b)$, on average over uniformly random $a, b \in \{0,1\}^m$.

Let $\hat{\tau}_R$ be as defined in the paragraph preceding the lemma. Note that $\hat{\tau}_R$ acts on $\mathcal{H}_{\mathsf{A}'}$ and $\mathcal{H}_{\hat{\mathsf{A}}}$. After application of the isometry, R has an expansion

$$R \simeq \hat{\tau}_R \cdot \Big(\sum_{a,b} \sigma_X(a)\sigma_Z(b) \otimes \Lambda_R(a,b) \Big),$$

for arbitrary $\Lambda_R(a,b)$ on $\mathcal{H}_{\hat{\mathsf{A}}}$; since $\hat{\tau}_R$ is invertible such an expansion exists for any operator. Using the approximate version of (4.11) certified by the conjugation test (Lemma 23),

$$R V_A^\dagger \big(\sigma_X(a)\sigma_Z(b) \otimes \Delta_Y^{a\cdot b}\big) V_A \approx V_A^\dagger \big(\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes \Delta_Y^{a\cdot b + h_S(a,b)}\big) V_A R,$$

where the approximation holds on average over a uniformly random choice of (a,b) and up to error that is polynomial in ε but independent of m. Expanding out R and using the consistency relations between the two provers,

$$\begin{aligned} \sum_{c,d} \hat{\tau}_R \Big(\sigma_X(c)\sigma_Z(d) \otimes \Lambda_R(c,d)\Big) \otimes \Big((-1)^{a\cdot b}\sigma_X(a)\sigma_Z(b) \otimes \Delta_Y^{a\cdot b}\Big) \\ \approx \sum_{c,d} \Big(\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes \Delta_Y^{a\cdot b + h_S(a,b)}\Big) \hat{\tau}_R \Big(\sigma_X(c)\sigma_Z(d) \otimes \Lambda_R(c,d)\Big) \otimes \mathbb{1}, \end{aligned} \tag{4.15}$$

where the factor $(-1)^{a\cdot b}$ comes from using

$$\big(\sigma_X(a)\sigma_Z(b) \otimes \mathbb{1}\big) |\mathrm{EPR}\rangle^{\otimes m} = \big(\mathbb{1} \otimes \big(\sigma_X(a)\sigma_Z(b)\big)^T\big) |\mathrm{EPR}\rangle^{\otimes m}.$$

Using the conjugation relations satisfied, by definition, by $\hat{\tau}_R$, the right-hand side of (4.15) simplifies to

$$\sum_{c,d} \hat{\tau}_R \Big(\sigma_X(a)\sigma_Z(b)\sigma_X(c)\sigma_Z(d) \otimes \Delta_Y^{a\cdot b}\Lambda_R(c,d)\Big) \otimes \mathbb{1}. \tag{4.16}$$

Next using the fact that the state on which the approximations are measured is maximally entangled across registers A and B, together with the Pauli (anti-)commutation relations, to simplify the left-hand side of (4.15), together with (4.16) we arrive at the approximation

$$\sum_{c,d} \Big((-1)^{a\cdot d + b\cdot c} \sigma_X(a+c)\sigma_Z(b+d) \otimes \Lambda_R(c,d) \Big) \otimes \Big(\mathbb{1} \otimes \Delta_Y^{a\cdot b} \Big) \\ \approx \sum_{c,d} \Big(\sigma_X(a+c)\sigma_Z(b+d) \otimes \Delta_Y^{a\cdot b} \Lambda_R(c,d) \Big) \otimes \mathbb{1}.$$

If $(c,d) \neq (0,0)$ a fraction about half of all (a,b) such that $a \cdot b = 0$ satisfy $a \cdot d + b \cdot c = 1$. Using that $\{\sigma_X(a)\sigma_Z(b) \otimes \mathbb{1} \, |\mathrm{EPR}\rangle\}$ are orthogonal for different (a,b), the above then implies that $\Lambda_R(c,d) \approx -\Lambda_R(c,d)$, on average over $(c,d) \neq (0,0)$. Hence $\Lambda_R(c,d) \approx 0$, on average over $(c,d) \neq (0,0)$. Considering (a,b) such that $a \cdot b = 1$ implies that $\Lambda_R(0,0)$ approximately commutes with Δ_Y. Finally, the relation (4.14) follows from self-consistency of X_R implicitly enforced in the test. □

4.4.3 Tensor products of single-qubit Clifford observables

We turn to testing observables in the m-fold direct product of the Clifford group. Although the test can be formulated more generally, for our purposes it will be sufficient to specialize it to the case where each element in the direct product is an observable taken from the set $\Sigma = \{X, Y, Z, F, G\}$ associated with the single-qubit Pauli observables defined in Section 4.2.2.1. Recall that the associated operators satisfy the conjugation relation $\sigma_Y \sigma_F \sigma_Y = \sigma_G$, which will be tested as part of our procedures (specifically, item (c) in Figure 4.8).

Test $\textsc{cliff}(\Sigma, m)$:

- Input: An integer m and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: Select $W \in \Sigma^m$ uniformly at random. Execute each of the following with equal probability:
  (a) Execute the test $\textsc{conj-cliff}(W)$;
  (b) Send one player either the query W, or X_W and the other $(W, X(e_{m+1}))$, where e_{m+1} indicates the control qubit used for part (a). Receive one bit from the first player, and two from the second. If the query to the first player was W, check that the first player's answer is consistent with the second player's first answer bit. If the query to the first player was X_W, then: If the second player's second bit is 0, check that his first bit is consistent with the first player's; If the second player's second bit is 1, check that his first bit is different than the first player's.
  (c) Let S and T be subsets of the positions in which $W_i = F$ and $W_i = G$ respectively, chosen uniformly at random. Let W' equal W except $W'_i = G$ for $i \in S$, and $W'_i = F$ for $i \in T$. Let $R = Y(\sum_{i \in S \cup T} e_i)$. Execute test $\textsc{conj}(W, W', R)$.
  (d) Set $W'_i = X$ (resp. Y) whenever $W_i = Y$ (resp. X), $W'_i = F$ (resp. G_i) whenever $W_i = G$ (resp. F), and $W'_i = X$ whenever $W_i = Z$. Execute test $\textsc{pbt}(W, W')$ on m qubits.
  (e) Let S and T be subsets of (non-overlapping) pairs of positions in which $W_i = F$ and $W_i = G$ respectively, chosen uniformly at random. Send one player the query W, with entries $(i, j) \in S \cup T$ removed and replaced by $\Phi_{i,j}$ (indicating a measurement in the Bell basis).
    - With probability $1/2$, send the other player the query W. Check consistency of outcomes associated with positions not in $S \cup T$. For outcomes in $S \cup T$, check the natural consistency as well: e.g. if the Bell measurement indicated the outcome Φ_{00}, then the two outcomes reported by the other player at those locations should be identical.
    - With probability $1/2$, execute an independent copy of the Bell measurement test $\textsc{Bell}$ (Figure 4.3) between the first and second players in each of the pair of qubits in $S \cup T$.

Figure 4.8: The m-qubit Clifford test, $\textsc{cliff}(\Sigma, m)$.

The test is described in Figure 4.8. It is divided in five parts. Part (a) of the test executes $\textsc{conj-cliff}(W)$ to verify that an observable $W \in \Sigma^m$ satisfies the appropriate Pauli conjugation relations (4.11). Note that a priori test $\textsc{conj-cliff}(W)$ only tests for the observable X_W obtained from W in blocks as X_R from R in (4.10) (indeed, in that test W need not be an observable). Thus part (b) of the test is introduced to verify that $X_W \approx WX(e_{m+1})$, where the $(m+1)$-st qubit is

the one used to specify the block decomposition relating X_W to W. The result of parts (a) and (b) is that, under the same isometry as used to specify the Pauli X and Z, $W \simeq \hat{\tau}_W \cdot (\mathbb{1} \otimes \Lambda_W)$, according to the same decomposition as shown in Lemma 25. The goal of the remaining three parts of the test is to verify that $\Lambda_W = \Lambda_F^{|\{i:W_i \in \{F,G\}\}|}$, for a single observable Λ_F. For this, part (c) of the test verifies that Λ_W only depends on the locations at which $W_i \in \{F, G\}$, but not on the specific observables at those locations. Part (d) verifies that $\Lambda_W \approx \prod_{i:W_i \in \{F,G\}} \Lambda_i$ for commuting observables Λ_i. Finally, part (e) checks that Λ_i is (approximately) independent of i.

Theorem 9. *Suppose a strategy for the players succeeds in test* CLIFF(Σ, m) *(Figure 4.8) with probability at least* $1 - \varepsilon$*. Then for* $D \in \{A, B\}$ *there exists an isometry*

$$V_D : \mathcal{H}_D \to (\mathbb{C}^2)_{D'}^{\otimes m} \otimes \mathcal{H}_{\hat{D}}$$

such that

$$\left\| (V_A \otimes V_B) \left|\psi\right\rangle_{AB} - \left|EPR\right\rangle_{A'B'}^{\otimes m} \left|AUX\right\rangle_{\hat{A}\hat{B}} \right\|^2 = O(\sqrt{\varepsilon}), \tag{4.17}$$

and

$$\mathbb{E}_{W \in \Sigma^m, c \in \{0,1\}^m} \left\| \mathbb{1}_A \otimes \left(V_B W(c) - \tau_W(c) V_B \right) \left|\psi\right\rangle_{AB} \right\|^2 = O(\mathrm{poly}(\varepsilon)). \tag{4.18}$$

Here τ_W *is defined from* W *as in Lemma 25, with* $\Lambda_{W_i} = \mathbb{1}$ *if* $W_i \in \{X, Y, Z\}$ *and* $\Lambda_{W_i} = \Lambda_F$ *if* $W_i \in \{F, G\}$*, where* Λ_F *is an observable on* $\mathcal{H}_{\hat{B}}$ *that commutes with* Δ_Y*.*

Proof sketch. The existence of the isometry, as well as (4.17) and (4.18) for $W \in \{I, X, Y, Z\}^m$, follows from the test PBT(X, Y, Z), executed as part of the Clifford conjugation test from part (a), and Lemma 24. Using part (a) of the test and Lemma 25 it follows that every $W \in \Sigma^m$ is mapped under the same isometry to

$$W \simeq_{\sqrt{\varepsilon}} \tau_W = \hat{\tau}_W (\mathbb{1} \otimes \Lambda_W), \tag{4.19}$$

where $\hat{\tau}_W$ is as defined in the lemma and Λ_W is an observable on $\mathcal{H}_{\hat{A}}$ which may depend on the whole string W; here we also use the consistency check in part (b) to relate the observable X_W used in the Clifford conjugation test with the observable W used in part (c). Note that from the definition we can write $\hat{\tau}_W = \otimes_i \hat{\tau}_{W_i}$, where in particular $\hat{\tau}_X = \sigma_X$, $\hat{\tau}_Z = \sigma_Z$ and $\hat{\tau}_Y = \sigma_Y \otimes \Delta_Y$.

The analysis of the conjugation test given in Lemma 23 shows that success with probability $1 - O(\varepsilon)$ in part (c) of the test implies the relations

$$\begin{aligned} \hat{\tau}_W \tau_R (\mathbb{1} \otimes \Lambda_W) &= \tau_R \hat{\tau}_W (\mathbb{1} \otimes \Lambda_W) \\ &\approx_{\sqrt{\varepsilon}} \hat{\tau}_{W'} \tau_R (\mathbb{1} \otimes \Lambda_{W'}), \end{aligned}$$

where the first equality is by definition of R, and uses that $\tau_Y = \sigma_Y \otimes \Delta_Y$ and Δ_Y commutes with Λ_W; the approximation holds as a consequence of the conjugation test and should be understood

on average over a uniformly random choice of $W \in \Sigma^m$. Thus Λ_W depends only on the locations at which $W_i \in \{F, G\}$, but not on the particular values of the observables at those locations.

Part (d) of the test and Lemma 24 imply that the observables $W(a)$ satisfy approximate linearity conditions $W(a)W(a') \approx W(a+a')$, on average over a uniformly random choice of $W \in \Sigma^n$ and $a, a' \in \{0,1\}^n$. Using the form (4.19) for W and the fact that the $\hat{\tau}_W(a)$ satisfy the linearity relations by definition, we deduce that $\Lambda_{W(a)}\Lambda_{W(a')} \approx \Lambda_{W(a+a')}$ as well. Using the analysis of the Pauli Braiding test (Lemma 24), this implies that for each i and W_i there is an observable Λ_{i,W_i} such that the Λ_{i,W_i} pairwise commute and $\Lambda_W \approx \prod_i \Lambda_{i,W_i}$. Using the preceding observations, $\Lambda_{i,W_i} \approx \Lambda_i$ if $W_i \in \{F, G\}$, and $\Lambda_{i,W_i} \approx \mathbb{1}$ if $W_i \in \{X, Y, Z\}$.

Success in part (e) of the test implies the condition $\mathbb{E}_W \langle\psi| W \otimes W_\Phi |\psi\rangle \geq 1 - O(\varepsilon)$, where W is distributed as in the test, and W_Φ is the observable applied by the second player upon a query W, with some locations, indexed by pairs in S and T, have been replaced by the Φ symbol (as described in the test). Let U be the set of i such that $W_i \in \{F, G\}$. Since Δ_Y commutes with all observables in play, for clarity let us assume in the following that $\Delta_Y = \mathbb{1}$. From the decomposition of the observables W obtained so far and the analysis of the test BELL given in Lemma 19 it follows that

$$W \simeq \Big(\otimes_i \hat{\tau}_{W_i}\Big) \otimes \Big(\prod_{i \in U} \Lambda_i\Big), \quad \text{and} \quad W_\Phi \simeq \Big(\otimes_{i \notin S \cup T} \hat{\tau}_{W_i}\Big) \otimes \Big(\otimes_{(i,j) \in S \cup T} \mathrm{SW}_{i,j}\Big) \otimes \Big(\prod_{i \in U \setminus S \cup T} \Lambda_i\Big),$$

where the ordering of tensor products does not respect the ordering of qubits, but it should be clear which registers each operator acts on. Using that for any operators A, B and Δ,

$$\langle \mathrm{EPR}|^{\otimes 2} \left(A \otimes B \otimes |\Phi_{00}\rangle\langle\Phi_{00}|\right) |\mathrm{EPR}\rangle^{\otimes 2} = \frac{1}{8} \operatorname{Tr}\left(AB^T\right),$$

the above conditions imply

$$\mathbb{E}_{S=\{(s_i,s_i')\}} \mathbb{E}_{T=\{(t_i,t_i')\}} \Lambda_{s_i}\Lambda_{s_i'}\Lambda_{t_i}\Lambda_{t_i'} \approx \mathbb{1},$$

where the expectation is taken over sets S and T specified as in part (e), for a given W, and on average over the choice of W. Let $\Lambda = \mathbb{E}_i \Lambda_i$. By an averaging argument it follows that for U the set of locations such that $W_i \in \{F, G\}$, $\prod_{i \in U} \Lambda_i \approx \Lambda^{|S|}$, again on average over the choice of W. To conclude we let $\Lambda_F = \Lambda/|\Lambda|$, which is an observable and satisfies the required conditions. □

4.4.4 Post-measurement states

We give a first corollary of Theorem 9 which expresses its conclusion (4.18) in terms of the post-measurement state of the first player. This corollary will be used in the analysis of the leash protocol from Section 4.5.2. To obtain a useful result we would like to "lift" the phase ambiguity Λ_W which remains in the statement of Theorem 9 (in contrast to the ambiguity Δ_Y, which itself cannot be

lifted solely by examining correlations). This ambiguity means that the provers have the liberty of choosing to report opposite outcomes whenever they apply an F or G observable, but they have to be consistent between themselves and across all of their qubits in doing so. To verify that the provers use the "right" labeling for their outcomes we incorporate a small tomography test in the test, described in Figure 4.9. Note that an inconvenience of the tomography is that the test no longer achieves perfect completeness (although completeness remains exponentially close to 1).

Test $\textsc{rigid}(\Sigma, m)$:

- Input: An integer m and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: execute each of the following with equal probability:
  (a) Execute the test $\textsc{cliff}(\Sigma, m)$;
  (b) Send each player a uniformly random query $W, W' \in \Sigma^m$. Let $T \subseteq \{1, \ldots, m\}$ be the subset of positions i such that $W_i \in \{X, Y\}$ and $W'_i \in \{F, G\}$. Reject if the fraction of answers (a_i, b_i), for $i \in T$, from the provers that satisfy the CHSH correlations (i.e. $a_i \neq b_i$ if and only if $(W_i, W'_i) = (X, F)$) is not at least $\cos^2 \frac{\pi}{8} - 0.1$.

Figure 4.9: The n-qubit rigidity test, $\textsc{rigid}(\Sigma, m)$.

For an observable $W \in \Sigma$, let $\sigma_W = \sigma_W^{+1} - \sigma_W^{-1}$ be its eigendecomposition, where σ_W are the "honest" Pauli matrices defined in (2.1) and (4.2). For $u \in \{\pm 1\}$ let $\sigma_{W,+} = \sigma_W^u$ for $W \in \Sigma$, and

$$\sigma_{X,-}^u = \sigma_X^u, \quad \sigma_{Z,-}^u = \sigma_Z^u, \quad \sigma_{Y,-}^u = \sigma_Y^{-u}, \quad \sigma_{F,-}^u = \sigma_G^{-u}, \quad \sigma_{G,-}^u = \sigma_F^{-u}.$$

Corollary 3. *Let $\varepsilon > 0$ and m an integer. Suppose a strategy for the players succeeds with probability $1 - \varepsilon$ in test $\textsc{rigid}(\Sigma, m)$. Then for $D \in \{A, B\}$ there exists an isometry*

$$V_D : \mathcal{H}_D \to (\mathbb{C}^2)_{D'}^{\otimes m} \otimes \mathcal{H}_{\hat{D}}$$

such that

$$\left\| (V_A \otimes V_B) \left| \psi \right\rangle_{AB} - \left| EPR \right\rangle^{\otimes m} \otimes \left| aux \right\rangle_{\hat{A}\hat{B}} \right\|^2 = O(\sqrt{\varepsilon}), \tag{4.20}$$

and positive semidefinite matrices τ_λ on $\hat{A}$ with orthogonal support, for $\lambda \in \{+, -\}$, such that $\mathrm{Tr}(\tau_+) + \mathrm{Tr}(\tau_-) = 1$ *and*

$$\begin{aligned} \mathop{E}_{W \in \Sigma^m} \sum_{u \in \{\pm 1\}^m} \left\| V_A \, \mathrm{Tr}_B \left((\mathbb{1}_A \otimes W_B^u) \left| \psi \right\rangle \left\langle \psi \right|_{AB} (\mathbb{1}_A \otimes W_B^u)^\dagger \right) V_A^\dagger - \sum_{\lambda \in \{\pm\}} \left(\bigotimes_{i=1}^m \frac{\sigma_{W_i,\lambda}^{u_i}}{2} \right) \otimes \tau_\lambda \right\|_1 \\ = O(\mathrm{poly}(\varepsilon)). \end{aligned} \tag{4.21}$$

Moreover, players employing the honest strategy succeed with probability $1 - e^{-\Omega(m)}$ in the test.

Proof. From Theorem 9 we get isometries V_A, V_B and commuting observables Δ_Y, Λ_F on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that the conclusions of the theorem hold. Write the eigendecomposition $\Delta_Y = \Delta_Y^+ - \Delta_Y^-$ and $\Lambda_F = \Lambda_F^+ - \Lambda_F^-$. For $\lambda \in \{+,-\}^2$ let

$$\tau_\lambda = \mathrm{Tr}_{\hat{\mathsf{B}}}\left(\left(\mathbb{1}_{\hat{\mathsf{A}}} \otimes \Delta_Y^{\lambda_1} \Lambda_F^{\lambda_2} \right) |\textsc{aux}\rangle\langle\textsc{aux}| \left(\mathbb{1}_{\hat{\mathsf{A}}} \otimes \Delta_Y^{\lambda_1} \Lambda_F^{\lambda_2} \right) \right).$$

Using that Δ_Y and Λ_F commute and satisfy

$$\Delta_Y \otimes \Delta_Y \, |\textsc{aux}\rangle \approx \Lambda_F \otimes \Lambda_F \, |\textsc{aux}\rangle \approx |\textsc{aux}\rangle$$

it follows that the (sub-normalized) densities τ_λ have (approximately) orthogonal support. In particular the provers' strategy in part (b) of the test is well-approximated by a mixture of four strategies, labeled by $(\lambda_Y, \lambda_F) \in \{\pm 1\}^2$, such that the strategy with label (λ_Y, λ_F) uses the observables

$$(X, Z, Y, F, G) \;=\; \Big(\sigma_X,\, \sigma_Z,\, \lambda_Y \sigma_Y,\, \frac{1}{\sqrt{2}} \lambda_F \big(-\sigma_X + \lambda_Y \sigma_Y \big),\, \frac{1}{\sqrt{2}} \lambda_F \big(\sigma_X + \lambda_Y \sigma_Y \big) \Big).$$

Among these four strategies, the two with $\lambda_F = -1$ fail part (b) of the test with probability exponentially close to 1. Success in both parts of the test with probability at least $1 - 2\varepsilon$ each thus implies

$$\mathrm{Tr}\left(\tau_{+-} \right) + \mathrm{Tr}\left(\tau_{--} \right) \;=\; \mathrm{poly}(\varepsilon). \tag{4.22}$$

For $W \in \Sigma^m$ and $c \in \{0,1\}^m$ the observable $W(c) = \otimes_i W_i^{c_i}$ can be expanded in terms of a 2^m-outcome projective measurement $\{W^u\}$ as

$$W(c) = \sum_{u \in \{0,1\}^m} (-1)^{u \cdot c} \, W^u.$$

Similarly, by definition we have that the projective measurement associated with the commuting Pauli observables $\tau_W(c) = \otimes_i \tau_{W_i}^{c_i}$, $c \in \{0,1\}^m$, is

$$\tau_W^u = \bigotimes_i \Big(\mathbb{E}_{c \in \{0,1\}^m} (-1)^{u \cdot c} \tau_W(c) \Big).$$

Thus,

$$\begin{aligned} &\mathbb{E}_{c \in \{0,1\}^m} \big\| \mathbb{1}_A \otimes \left(W(c) - V_B^\dagger \tau_W(c) V_B \right) |\psi\rangle_{\mathsf{AB}} \big\|^2 \\ &\qquad = \mathbb{E}_{c \in \{0,1\}^m} \Big\| \sum_u (-1)^{u \cdot c} \mathbb{1}_A \otimes \left(W^u - V_B^\dagger \tau_W^u V_B \right) |\psi\rangle_{\mathsf{AB}} \Big\|^2 \\ &\qquad = \sum_{u \in \{0,1\}^m} \big\| \mathbb{1}_A \otimes \left(W^u - V_B^\dagger \tau_W^u V_B \right) |\psi\rangle_{\mathsf{AB}} \big\|^2, \end{aligned} \tag{4.23}$$

where the third line is obtained by expanding the square and using $\mathbb{E}_{c\in\{0,1\}^m}(-1)^{v\cdot c} = 1$ if $v = 0^m$, and 0 otherwise. Using (4.18), the expression in (4.23), when averaged over all $W \in \Sigma^m$, is bounded by $O(\mathrm{poly}(\varepsilon))$. Using the Fuchs-van de Graaf inequality and the fact that trace distance cannot increase under tracing out, we get that the following is $O(\mathrm{poly}(\varepsilon))$:

$$\mathbb{E}_{W\in\Sigma^m}\sum_u \left\| V_A \,\mathrm{Tr}_{\mathsf{B}}\left((\mathbb{1}_{\mathsf{A}}\otimes W^u)\,|\psi\rangle\langle\psi|\,(\mathbb{1}_{\mathsf{A}}\otimes W^u)^\dagger\right)V_A^\dagger - \mathrm{Tr}_{\mathsf{B}}\left((\mathbb{1}_{\mathsf{A}}\otimes \tau_W^u)\,|\psi\rangle\langle\psi|\,(\mathbb{1}_{\mathsf{A}}\otimes \tau_W^u)^\dagger\right)\right\|_1. \tag{4.24}$$

Using that $\tau_X = \sigma_X$, $\tau_Z = \sigma_Z$, and $\tau_Y = \sigma_Y\Delta_Y$, we deduce the post-measurement states for $u \in \{\pm 1\}$

$$\tau_X^u = \sigma_X^u, \qquad \tau_Z^u = \sigma_Z^u, \qquad \tau_Y^u = \sigma_Y^u \otimes (\tau_{++} + \tau_{+-}) + \sigma_Y^{-u} \otimes (\tau_{-+} + \tau_{--}).$$

Similarly, from $\tau_F = (-\tau_X + \tau_Y)\Lambda_F$ and $\tau_G = (\tau_X + \tau_Y)\Lambda_F$ we get that e.g. the $+1$ eigenspace of τ_F is the combination of:

- The simultaneous $+1$ eigenspace of $\sigma_F = (-\sigma_X + \sigma_Y)/\sqrt{2}$, $+1$ eigenspace of Δ_Y, and $+1$ eigenspace of Λ_F;
- The simultaneous -1 eigenspace of σ_F, $+1$ eigenspace of Δ_Y, and -1 eigenspace of Λ_F;
- The simultaneous -1 eigenspace of $\sigma_G = -(-\sigma_X - \sigma_Y)/\sqrt{2}$, -1 eigenspace of Δ_Y, and $+1$ eigenspace of Λ_F;
- The simultaneous $+1$ eigenspace of σ_G, -1 eigenspace of Δ_Y, and -1 eigenspace of Λ_F.

Proceeding similarly with τ_G, we obtain

$$\begin{aligned}\tau_F^u &= \sigma_F^u \otimes \tau_{++} + \sigma_F^{-u} \otimes \tau_{+-} + \sigma_G^{-u} \otimes \tau_{-+} + \sigma_G^u \otimes \tau_{--},\\ \tau_G^u &= \sigma_G^u \otimes \tau_{++} + \sigma_G^{-u} \otimes \tau_{+-} + \sigma_F^{-u} \otimes \tau_{-+} + \sigma_F^u \otimes \tau_{--}.\end{aligned}$$

Starting from (4.24) and using (4.17) we obtain

$$\begin{aligned}\mathbb{E}_{W\in\Sigma^m}\sum_u \Big\| V_A \,\mathrm{Tr}_{\mathsf{B}}&\left((\mathbb{1}_{\mathsf{A}}\otimes W^u)\,|\psi\rangle\langle\psi|\,(\mathbb{1}_{\mathsf{A}}\otimes W^u)^\dagger\right)V_A^\dagger\\ &- \mathrm{Tr}_{\mathsf{B}}\left((\mathbb{1}_{\mathsf{A}}\otimes \tau_W^u)\,|\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes m}\otimes|\mathrm{AUX}\rangle\langle\mathrm{AUX}|_{\hat{\mathsf{A}}\hat{\mathsf{B}}}\,(\mathbb{1}_{\mathsf{A}}\otimes \tau_W^u)^\dagger\right)\Big\|_1 = O(\mathrm{poly}(\varepsilon)).\end{aligned}$$

Since $\mathrm{Tr}_{\mathsf{B}}(\mathbb{1}\otimes B\,|\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{\mathsf{AB}}\,\mathbb{1}\otimes B^\dagger) = (B^\dagger B)^T/2$ for any single-qubit operator B, to conclude the bound claimed in the theorem it only remains to apply the calculations above and use (4.22) to eliminate the contribution of τ_{+-} and τ_{--}; the factor $\frac{1}{2}$ comes from the reduced density matrix of an EPR pair. □

4.4.5 Tomography

Theorem 9 and Corollary 3 show that success in test $\textsc{rigid}(\Sigma, m)$ gives us control over the players' observables and post-measurement states in the test. This allows us to use one of the players to perform some kind of limited tomography (limited to post-measurement states obtained from measurements in Σ), that will be useful for our analysis of the Dog-Walker Protocol from Section 4.5.3.

Let $1 \leq m' \leq m$ and consider the test $\textsc{tom}(\Sigma, m', m)$ described in Figure 4.10. In this test, one player is sent a question $W \in \Sigma^m$ chosen uniformly at random. Assuming the players are also successful in the test $\textsc{rigid}(\Sigma, m)$ (which can be checked independently, with some probability), using that the input distribution μ in $\textsc{rigid}(\Sigma, m)$ assigns weight at least $|\Sigma|^{-m}/2$ to any $W' \in \Sigma^m$, from Corollary 3 it follows that the second player's post-measurement state is close to a state consistent with the first player's reported outcomes. Now suppose the second player is sent a random subset $S \subseteq [m]$ of size $|S| = m'$, and is allowed to report an arbitrary string $W' \in \Sigma^{m'}$, together with outcomes u. Suppose also that for each $i \in S$, we require that $u_i = a_i$ whenever $W'_i = W_i$. Since the latter condition is satisfied by a constant fraction of $i \in \{1, \ldots, m'\}$, irrespective of W', with very high probability, it follows that the only possibility for the second player to satisfy the condition is to actually measure his qubits precisely in the basis that he indicates. This allows us to check that a player performs the measurement that he claims, even if the player has the choice of which measurement to report.

Tomography Test $\textsc{tom}(\Sigma, m', m)$:

- Input: Integer $1 \leq m' \leq m$ and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: Let $S \subseteq [m]$ be chosen uniformly at random among all sets of size $|S| = m'$. Select $W \in \Sigma^m$ uniformly at random. Send W to the first player, and the set S to the second. Receive a from the first player, and $W' \in \Sigma^{m'}$ and u from the second. Accept only if $a_i = u_i$ whenever $i \in S$ and $W_i = W'_i$.

Figure 4.10: The m-qubit tomography test $\textsc{tom}(\Sigma, m', m)$.

Corollary 4. *Let $\varepsilon > 0$ and $1 \leq m' \leq m$ integer. Suppose a strategy for the players succeeds with probability $1 - \varepsilon$ in both tests $\textsc{rigid}(\Sigma, m)$ (Figure 4.9) and $\textsc{tom}(\Sigma, m', m)$ (Figure 4.10). Let V_A, V_B be the isometries specified in Corollary 3. Let $\{Q^{W',u}\}$ be the projective measurement applied by the second player in $\textsc{tom}(\Sigma, m', m)$. Then there exists a distribution q on $\Sigma^{m'} \times \{\pm\}$*

such that

$$\sum_{W'\in\Sigma^{m'}}\sum_{u\in\{\pm 1\}^{m'}}\Big\|\operatorname{Tr}_{A\hat{B}}\left((\mathbb{1}_A\otimes V_B Q^{W',u})\,|\psi\rangle\langle\psi|_{AB}\,(\mathbb{1}_A\otimes V_B Q^{W',u})^\dagger\right) - \sum_{\lambda\in\{\pm\}} q(W',\lambda)\Big(\bigotimes_{i=1}^{m'}\frac{1}{2}\sigma^{u_i}_{W'_i,\lambda}\Big)\Big\|_1 = O(\mathrm{poly}(\varepsilon)),$$

where the notation is the same as in Corollary 3.

Moreover, players employing the honest strategy succeed with probability 1 *in tomography part of the test.*

Proof. Success in $\textsc{rigid}(\Sigma,m)$ allows us to apply Corollary 3. For any (W',u) let $\rho^{W',u}_{\mathsf{A}',\lambda}$ be the post-measurement state on the first player's space, conditioned on the second player's answer in $\textsc{tom}(\Sigma,m',m)$ being (W',u), after application of the isometry V_A, and conditioned on $\mathcal{H}_{\hat{\mathsf{A}}}$ being in a state that lies in the support of τ_λ (note this makes sense since τ_+, τ_- have orthogonal support). Using that for any $i\in S$, $W_i = W'_i$ with constant probability $|\Sigma|^{-1}$, it follows from (4.20) and (4.21) in Corollary 3 that success in $\textsc{tom}(\Sigma,m)$ implies the condition

$$\mathop{\mathbb{E}}_{\substack{S\subseteq\{1,\ldots,m\}\\|S|=m'}}\sum_{W',\lambda,u}\operatorname{Tr}(\tau_\lambda)\,\operatorname{Tr}\Big(\Big(\frac{|\Sigma|-1}{|\Sigma|}\mathbb{1}+\frac{1}{|\Sigma|}\otimes_{i\in S}\sigma^{u_i}_{W'_i,\lambda}\Big)\rho^{W',u}_{\mathsf{A}',\lambda}\Big) = 1-O(\mathrm{poly}(\varepsilon)). \quad (4.25)$$

Eq (4.25) concludes the proof, for some distribution $q(W',\lambda)\approx\sum_u \operatorname{Tr}\Big(\rho^{W',u}_{\mathsf{A}',\lambda}\Big)\operatorname{Tr}(\tau_\lambda)$ (the approximation is due to the fact that the latter expression only specifies a distribution up to error $O(\mathrm{poly}(\varepsilon))$. □

4.5 Delegating a quantum computation

We are finally ready to describe our new delegation protocols.

4.5.1 Preliminaries

4.5.1.1 Quantum circuits

We use capital letters in sans-serif font to denote gates. We work with the universal quantum gate set $\{\mathsf{CNOT}, \mathsf{H}, \mathsf{T}\}$, where the controlled-not gate is the two-qubit gate with the unitary action

$$\mathsf{CNOT} \left|b_1, b_2\right\rangle = \left|b_1, b_1 \oplus b_2\right\rangle,$$

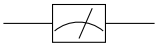
and the Hadamard and T gates are single-qubit gates with actions

$$\mathsf{H} \left|b\right\rangle = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle + (-1)^b \left|1\right\rangle\right) \text{ and } \mathsf{T} \left|b\right\rangle = e^{ib\pi/4} \left|b\right\rangle,$$

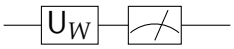
respectively. We will also use the following gates:

$$\mathsf{X} \left|b\right\rangle = \left|b \oplus 1\right\rangle, \ \mathsf{Z} \left|b\right\rangle = (-1)^b \left|b\right\rangle, \text{ and } \mathsf{P} \left|b\right\rangle = i^b \left|b\right\rangle.$$

Measurements in the Z basis (or computational basis) will be denoted by the standard measurement symbol:



To measure another observable, W, we can perform a unitary change of basis U_W, so that the following circuit meaures in the eigenbasis of W:



We assume that every circuit has a specified output wire, which is measured at the end of the computation to obtain the output bit. Without loss of generality, we can assume this is always the first wire. For an n-qubit system, we let Π_b, for $b \in \{0,1\}$, denote the orthogonal projector onto states with $\left|b\right\rangle$ in the output wire: $\left|b\right\rangle\left\langle b\right| \otimes \mathbb{1}$. For example, the probability that a circuit Q outputs 0 on input $\left|\mathbf{x}\right\rangle$ is $\left\|\Pi_0 Q \left|\mathbf{x}\right\rangle\right\|^2$.

We can always decompose a quantum circuit into layers such that each layer contains at most one T gate applied to each wire. The minimum number of layers for which this is possible is called the T *depth* of the circuit. We note that throughout this work we will assume circuits are compiled in a specific form that introduces extra T gates (see the paragraph on the H gadget in Section 4.5.1.2). The T depth of the resulting circuit is proportional to the depth of the original circuit.

4.5.1.2 Broadbent's EPR Protocol

In this section we summarize the main features of a delegation protocol introduced in [11], highlighting the aspects that will be relevant to understanding our subsequent adaptation into two-prover protocols. The "EPR Protocol" from [11] involves the interaction between a verifier V_{EPR} and a prover P. We write P_{EPR} for the "honest" behavior of the prover. The verifier V_{EPR} has limited quantum powers. Her goal is to delegate a BQP computation to the prover P in a verifiable way. Specifically, the verifier has as input a quantum circuit Q on n qubits and an input string $\mathbf{x} \in \{0,1\}^n$, and the prover gets as input Q. The verifier and prover interact. At the end of the protocol, the verifier outputs either a*ccept* or r*eject*. The protocol is such that there exist values p_{sound} and p_{compl} with $p_{\text{sound}} < p_{\text{compl}}$ such that $p_{\text{compl}} - p_{\text{sound}}$, called the *soundness-completeness gap*, is a constant independent of input size, and moreover:

Completeness: If the prover is honest and $\|\Pi_0 Q|\mathbf{x}\rangle\|^2 \geq 2/3$, then the verifier outputs a*ccept* with probability at least p_{compl};

Soundness: If $\|\Pi_0 Q|\mathbf{x}\rangle\|^2 \leq 1/3$, then the probability the verifier outputs a*ccept* is at most p_{sound}.

In Section 4.5.4, we show that sequential repetition can be used to turn any such protocol, including our two-prover variants, into one in which the verifier outputs 0, 1, or a*bort*, and we have the following: (1) If the prover(s) is/are honest, the verifier outputs a*bort* with probability at most .01; and (2) If $\|\Pi_b Q|\mathbf{x}\rangle\|^2 \geq 2/3$ for some $b \in \{0,1\}$ then the probability that the verifier outputs $1-b$ is at most .01.

In the EPR protocol, V_{EPR} and P_{EPR} are assumed to share $(n+t)$ EPR pairs at the start of the protocol, where t is the number of T gates in Q and n the number of input bits. (In [11] the EPR protocol is only considered in the analysis, and it is assumed that the EPR pairs are prepared by the verifier.) The first n EPR pairs correspond to the input to the computation; they are indexed by $N = \{1,\ldots,n\}$. The remaining pairs are indexed by $T = \{n+1,\ldots,n+t\}$; they will be used as ancilla qubits to implement each of the T gates in the delegated circuit.

The behavior of V_{EPR} depends on a *round type* randomly chosen by V_{EPR} after her interaction with P_{EPR}. There are three possible round types:

- Computation round ($r = 0$): the verifier delegates the computation to P_{EPR}, and at the end of the round can recover its output if P_{EPR} behaves honestly;
- X-test round ($r = 1$) and Z-test round ($r = 2$): the verifier tests that P_{EPR} behaves honestly, and rejects if malicious behavior is detected.

For some constant p, V chooses $r = 0$ with probability p, and otherwise chooses $r \in \{1,2\}$ with equal probability. Since the choice of round type is made after interaction with P_{EPR}, P_{EPR}'s behavior cannot depend on the round type. In particular, any deviating behavior in a computation round is reproduced in both types of test rounds. The analysis amounts to showing that any deviating behavior that affects the outcome of the computation will be detected in at least one of the test rounds.

In slightly more detail, the high-level structure of the protocol is the following. V_{EPR} measures her halves of the n qubits in N in order to prepare the input state on P_{EPR}'s system. As a result the input is quantum one-time padded with keys that depend on V_{EPR}'s measurement results. For example, in a computation round, V_{EPR} measures each input qubit in the Z basis, and gets some result $\mathbf{d} \in \{0,1\}^n$, meaning the input on P_{EPR}'s side has been prepared as $\mathsf{X}^{\mathbf{d}} |0\rangle^{\otimes n}$. In [11], the input is always considered to be $\mathbf{0}$, but we can also prepare an arbitrary classical input $\mathbf{x} \in \{0,1\}^n$ by reinterpreting the one-time pad key as $\mathbf{a} = \mathbf{d} \oplus \mathbf{x}$ so that the input state on P_{EPR}'s side is $\mathsf{X}^{\mathbf{a}} |\mathbf{x}\rangle$. In a test round, on the other hand, the input is prepared as the one-time pad of either $|0\rangle^{\otimes n}$ or $|+\rangle^{\otimes n}$. Note that as indicated in Figure 4.12 this choice of measurements will be made after the interaction with P_{EPR} has taken place.

The honest prover P_{EPR} applies the circuit Q, which we assume is compiled in the universal gate set $\{\mathsf{H}, \mathsf{T}, \mathsf{C}NOT\}$, to his one-time padded input. We will shortly describe gadgets that P_{EPR} can apply in order to implement each of the three gate types. The gadgets are designed in a way that in a test round each gadget amounts to an application of an identity gate; this is what enables V_{EPR} to perform certain tests in those rounds that are meant to identify deviating behavior of a dishonest prover. After each gadget, the one-time padded keys can be updated by V_{EPR}, who is able to keep track of the keys at any point in the circuit using the *update rules* in Table 4.2. We now describe the three gadgets, before giving a complete description of the protocol.

4.5.1.3 CNOT Gadget

To implement a $\mathsf{C}NOT$ gate on wires j and j', P_{EPR} simply performs the $\mathsf{C}NOT$ gate on those wires of his input qubits. The one-time pad keys are changed by the update rule in Table 4.2, because $\mathsf{C}NOT \cdot \mathsf{X}^{a_j}\mathsf{Z}^{b_j} \otimes \mathsf{X}^{a_{j'}}\mathsf{Z}^{b_{j'}} = \mathsf{X}^{a_j}\mathsf{Z}^{b_j+b_{j'}} \otimes \mathsf{X}^{a_j+a_{j'}}\mathsf{Z}^{b_{j'}} \cdot \mathsf{C}NOT$. Note that $\mathsf{C}NOT |0\rangle |0\rangle = |0\rangle |0\rangle$ and $\mathsf{C}NOT |+\rangle |+\rangle = |+\rangle |+\rangle$, so in the test runs, P_{EPR} is applying the identity.

4.5.1.4 H Gadget

To implement an H gate on wire j, P_{EPR} simply performs the H on wire j, and the one-time-pad keys are changed as in Table 4.2. Unlike $\mathsf{C}NOT$, H does not act as the identity on $|0\rangle$ and $|+\rangle$, so it is not the identity in a test round. To remedy this, assume that Q is compiled so that every H

		Key Update Rule
T	Computation Round	$(a_j, b_j) \leftarrow (a_j + c_i, b_j + e_i + a_j + c_i + (a_j + c_i)z_i)$
	X-Test, even parity; or Z-test, odd parity	$(a_j, b_j) \leftarrow (e_i, 0)$
	Z-Test, even parity; or X-test, odd parity	$(a_j, b_j) \leftarrow (0, b_j + e_i + z_i)$
H		$(a_j, b_j) \leftarrow (b_j, a_j)$
$CNOT$		$(a_j, b_j, a_{j'}, b_{j'}) \leftarrow (a_j, b_j + b_{j'}, a_j + a_{j'}, b_{j'})$

Table 4.2: Rules for updating the one-time-pad keys after applying each type of gate in the EPR Protocol, in particular: after applying the i-th T gate to the j-th wire; applying an H gate to the j-th wire; or applying a $CNOT$ gate controlled on the j-th wire and targeting the j'-th wire.

gate appears in a pattern $\mathsf{H}(\mathsf{T}TH)^k$, where the maximal such k is odd. This can be accomplished by replacing each H by $\mathsf{H}TTHTTHTTH$, which implements the same unitary. In test rounds, the T gadget, described shortly, implements the identity, and since $\mathsf{H}(\mathbb{1}\mathsf{H})^k$ for odd k implements the identity, $\mathsf{H}(\mathsf{T}TH)^k$ will also have no effect in test rounds.

4.5.1.5 Parity of a T Gate

Within a pattern $\mathsf{H}(\mathsf{T}TH)^k$, the H has the effect of switching between an X-test round scenario (the state $|0\rangle$) and a Z-test round scenario (the state $|+\rangle$). In order to consistently talk about the type of a round while evaluating the circuit, we can associate a parity with each T gate in the circuit. The parity of the T gates that are not part of the pattern $\mathsf{H}(\mathsf{T}TH)^k$ will be defined to be even. A H will always flip the parity, so that within such a pattern, the first two T gates will be odd, the next two will be even, etc., until the last two T gates will be odd again.

4.5.1.6 T Gadget

The gadget for implementing the i-th T gate on the j-th wire is performed on P_{EPR}'s j-th input qubit, and his i-th auxiliary qubit (indexed by $n + i$), which we can think of as being prepared in a particular auxiliary state by V_{EPR} measuring her half of the corresponding EPR pair, as shown in Figure 4.11. The gadget depends on a random bit z_i that is chosen by V_{EPR} and sent to the prover.

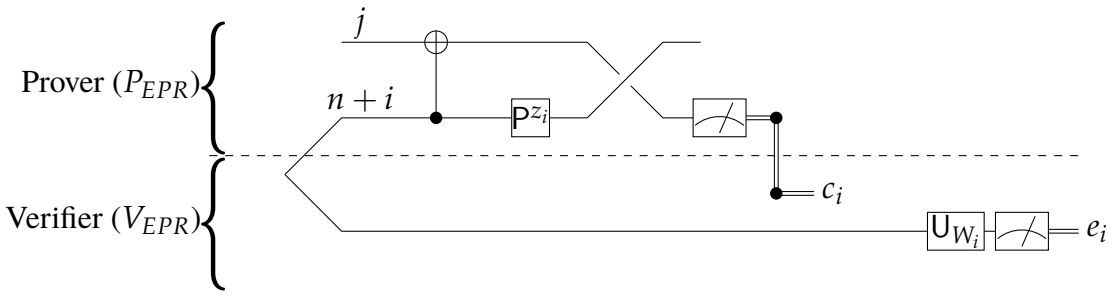


Figure 4.11: The gadget for implementing the i-th T gate on the j-th wire. The gate U_{W_i} implementing the change of basis associated with observable W_i is applied as part of the procedure V^r_{EPR} (see Figure 4.14) and is determined by the round type r, the parity of the i-th T gate, z_i, c_i, and a'_i (the X-key going into the i-th T gate), as in Table 4.3.

			U_{W_i} (observable W_i)
Computation Round	$a'_i \oplus c_i \oplus z_i = 0$		$\mathsf{H}T$ (observable G)
	$a'_i \oplus c_i \oplus z_i = 1$		$\mathsf{H}PT$ (observable F)
X-Test Round	even T gate		$\mathbb{1}$ (observable Z)
	odd T gate	$z_i = 0$	H (observable X)
		$z_i = 1$	$\mathsf{H}P$ (observable Y)
Z-Test Round	odd T gate		$\mathbb{1}$ (observable Z)
	even T gate	$z_i = 0$	H (observable X)
		$z_i = 1$	$\mathsf{H}P$ (observable Y)

Table 4.3: The choice of U_{W_i} in the T gadget. We also indicate the observable W_i associated with the final measurement $W_i = \mathsf{U}^\dagger_{W_i} Z \mathsf{U}_{W_i}$.

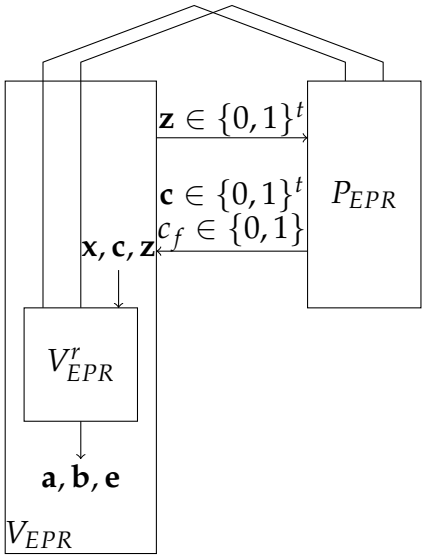


Figure 4.12: This figure describes how different pieces of the protocol fit together. V_{EPR} and P_{EPR} share $n+t$ EPR pairs. The honest prover P_{EPR} can be seen as a procedure that acts on $n+t$ qubits — the EPR pair halves — depending on a t-bit string $\mathbf{z}$. We have separated the quantum part of V_{EPR} into its own procedure, called V^r_{EPR}, where $r \in \{0,1,2\}$ indicates the *round type*, which V_{EPR} runs on her $n+t$ EPR halves, and the $2t$ bits $\mathbf{c}$ and $\mathbf{z}$. Aside from running V^r_{EPR}, V_{EPR} is classical.

4.5.1.7 The EPR Protocol.

We show how the gadgets just described are used in the complete protocol. We first describe the protocol for V_{EPR} below. For later convenience we have divided the action of V_{EPR} into classical actions and a single quantum subroutine V_{EPR}^r depending on the round type.

---

1. V_{EPR} chooses $\mathbf{z} \in_R \{0,1\}^t$, sends it to P_{EPR},[a] and receives back $\mathbf{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$.
2. V_{EPR} chooses a random round type $r \in \{0,1,2\}$ and runs V_{EPR}^r (see Figure 4.14) on her EPR halves, $\mathbf{x}$, $\mathbf{c}$ and $\mathbf{z}$, to obtain bits $\mathbf{a}, \mathbf{b} \in \{0,1\}^n$ and $\mathbf{e} \in \{0,1\}^t$.
3. V_{EPR} applies the update rules from Table 4.2 on the initial keys $(\mathbf{a}, \mathbf{b})$, gate-by-gate, to obtain, for every $i \in [t]$, the X-key before the i-th T gate is applied, a'_i, and the final X key for the output wire, a'_f. If $r = 1$ (X-test round) and there exists an i such that the i-th T gate is even and $c_i \neq a'_i \oplus e_i$, output *reject*. If $r = 2$ (Z-test round) and there exists an i such that the i-th T gate is odd and $c_i \neq a'_i \oplus e_i$, output *reject*. If $r \in \{0,1\}$ (computation or X-test round) and $c_f \oplus a'_f \neq 0$, output *reject*. Otherwise, output *accept*.

Figure 4.13: The EPR Protocol: V_{EPR}'s point of view.

[a] We note that in the original EPR Protocol of [11], this is accomplished by P_{EPR} and V_{EPR} both measuring t EPR pairs in the Z basis to get a shared random string $\mathbf{z}$.

The procedure V_{EPR}^r measures each of the $n + t$ EPR halves according to some observable that depends on r, $\mathbf{c}$, and $\mathbf{z}$. In the case of a computation round, V_{EPR}^0 measures the qubits in T adaptively.

Input: A circuit Q with t T gates, $\mathbf{x} \in \{0,1\}^n$, $\mathbf{c}, \mathbf{z} \in \{0,1\}^t$, an n-qubit system indexed by N, and a t-qubit system indexed by T.

1. If $r \in \{0,1\}$, measure each qubit in N in the Z basis, and otherwise measure in the X basis, to get results $\mathbf{d} \in \{0,1\}^n$. If $r = 0$, set $(\mathbf{a}, \mathbf{b}) = (\mathbf{d} \oplus \mathbf{x}, 0^n)$; if $r = 1$, set $(\mathbf{a}, \mathbf{b}) = (\mathbf{d}, 0^n)$; and if $r = 2$ set $(\mathbf{a}, \mathbf{b}) = (0^n, \mathbf{d})$.
2. Going through Q gate-by-gate, use the update rules in Table 4.2 to update the one-time-pad keys. For every $i \in [t]$, when the i-th T gate is reached, let a'_i be the X key before the i-th T gate is applied. Choose an observable W_i according to Table 4.3 in which to measure the i-th qubit in T, corresponding to the i-th T gate, obtaining result e_i.

Figure 4.14: The procedure V_{EPR}^r, employed by V_{EPR}.

Finally, we describe the behavior of an honest prover, P_{EPR}.

1. Receive $\mathbf{z} \in \{0,1\}^t$ from V_{EPR}.
2. Evaluate Q gate-by-gate using the appropriate gadget for each gate. In particular, use z_i to implement the i-th T gadget, and obtain measurement result c_i.
3. Measure the output qubit to obtain c_f, and return $\mathbf{c}$ and c_f to V_{EPR}.

Figure 4.15: The EPR Protocol: Honest prover strategy P_{EPR}.

4.5.1.8 Completeness and Soundness.

We summarize the relevant part of the analysis of the EPR protocol from [11]. First suppose P_{EPR} behaves honestly. If $\|\Pi_0 Q\,|0^n\rangle\|^2 = p$, then in a computation round, V_{EPR} outputs a*ccept* with probability p, whereas in a test round, V_{EPR} outputs a*ccept* with probability 1. This establishes completeness of the protocol:

Theorem 10 (Completeness)**.** *Suppose the verifier executes the EPR Protocol, choosing $r = 0$ with probability p, on an input $(Q, |\mathbf{x}\rangle)$ such that $\|\Pi_0 Q\,|\mathbf{x}\rangle\|^2 \geq 1-\delta$. Then the probability that V_{EPR} accepts when interacting with the honest prover P_{EPR} is at least $(1-p)+p(1-\delta)$.*

The following theorem is implicit in [11, Section 7.6], but we include a brief proof sketch:

Theorem 11 (Soundness)**.** *Suppose the verifier executes the EPR Protocol, choosing $r = 0$ with probability p, on an input $(Q, |\mathbf{x}\rangle)$ such that $\|\Pi_0 Q\,|\mathbf{x}\rangle\|^2 \leq \delta$. Let P^*_{EPR} be an arbitrary prover such that P^*_{EPR} is accepted by V_{EPR} with probability q_t conditioned on $r \neq 0$, and q_c conditioned on $r = 0$. Then the prover's overall acceptance probability is $pq_c + (1-p)q_t$, and*

$$q_c \;\leq\; 2\,(q_t\,\delta + (1-q_t)) - \delta.$$

Proof sketch. Using the notation of [11], let $A = \sum_k \sum_{Q \in B'_{t,n}} |\alpha_{k,Q}|^2$. For intuition, A should be thought of as the total weight on attacks that could change the outcome of the computation, called non-benign attacks in [11]. By [11], the probability of rejecting in a computation round is $1 - q_c \geq (1-\delta)(1-A)$, whereas the probability of rejecting in a test round is $1 - q_t \geq \frac{1}{2}A$. Combining these gives $q_c \leq 2(q_t\delta + (1-q_t)) - \delta$. □

4.5.2 The Verifier-on-a-Leash Protocol

4.5.2.1 Protocol and statement of results

The Verifier-on-a-Leash Protocol (or "Leash Protocol" for short) involves a classical verifier and two quantum provers. The idea behind the Leash Protocol is to have a first prover, nicknamed PV

for Prover V, carry out the quantum part of V_{EPR} from Broadbent's EPR Protocol by implementing the procedure V_{EPR}^r. (See Section 4.5.1.2 for a summary of the protocol and a description of V_{EPR}. Throughout this section we assume that the circuit Q provided as input is compiled in the format described in Section 4.5.1.2.). A second prover, nicknamed PP for Prover P, will play the part of the prover P_{EPR}. Unlike in the EPR Protocol, the interaction with PV (i.e. running V_{EPR}^r) will take place first, and PV will be asked to perform random measurements from the set $\Sigma = \{X, Y, Z, F, G\}$. The values $\mathbf{z}$, rather than being chosen at random, will be chosen based on the corresponding choice of observable. We let n be the number of input bits and t number of T gates in Q.

The protocol is divided into two sub-games; which game is played is chosen by the verifier by flipping a biased coin with probability $(p_r, p_d = 1 - p_r)$.

- The first game is a sequential version of the rigidity game $\textsc{rigid}(\Sigma, m)$ (from Section 4.4) described in Figure 4.21. This aims to enforce that PV performs precisely the right measurements;
- The second game is the delegation game, described in Figures 4.18, 4.19, and 4.20, and whose structure is summarized in Figure 4.16. Here the verifier guides PP through the computation in a similar way as in the EPR Protocol.

We call the resulting protocol the Leash Protocol with parameters (p_r, p_d). In both sub-games the parameter $m = \Theta(n + t)$ is chosen large enough so that with probability close to 1 each symbol in Σ appears in a random $W \in \Sigma^m$ at least $n + t$ times. It is important that PV is not able to tell which kind of game is being played. Notice also that in order to ensure blindness, we will require that the interaction with PV in the delegation game is sequential (more details on this are found in Section 4.5.2.4). In order for the two sub-games to be indistinguishable, we also require that the rigidity game $\textsc{rigid}(\Sigma, m)$ be played sequentially (i.e. certain subsets of questions and answers are exchanged sequentially, but the acceptance condition in the test is the same). Note, importantly, that the rigidity guarantees of $\textsc{rigid}(\Sigma, m)$ from Section 4.4 hold verbatim when the game is played sequentially, since this only reduces the number of ways that the provers can cheat. The following theorem states the guarantees of the Leash Protocol.

Theorem 12. *There are constants $p_r, p_d = 1 - p_r$, and $\Delta > 0$ such that the following hold of the Verifier-on-a-Leash Protocol with parameters (p_r, p_d), when executed on an input $(Q, |\mathbf{x}\rangle)$.*

- (Completeness:) *Suppose that $\|\Pi_0 Q |\mathbf{x}\rangle\|^2 \geq 2/3$. Then there is a strategy for PV and PP that is accepted with probability at least $p_{\text{compl}} = p_r(1 - e^{-\Omega(n+t)}) + 8p_d/9$.*

- (Soundness:) *Suppose that* $\|\Pi_0 Q\,|\mathbf{x}\rangle\,\|^2 \leq 1/3$. *Then any strategy for PV and PP is accepted with probability at most* $p_{\text{sound}} = p_{\text{compl}} - \Delta$.

Further, the protocol leaks no information about $\mathbf{x}$ *to either prover individually, aside from an upper bound on the length of* $\mathbf{x}$.

The proof of the completeness property is given in Lemma 26. The soundness property is shown in Lemma 29. Blindness is established in Section 4.5.2.4. We first give a detailed description of the protocol. We start by describing the delegation game, specified in Figures 4.18, 4.19 and 4.20, which describe the protocol from the verifier's view, an honest PV's view, and an honest PP's view respectively. This will motivate the need for a sequential version of the game $\textsc{rigid}(\Sigma, m)$, described in Figure 4.21. As we will show, the rigidity game forces PV to behave honestly. Thus, for the purpose of exposition, we assume for now that PV behaves honestly, which results in the joint behavior of PV and V being similar to that of the verifier V_{EPR} in the EPR Protocol.

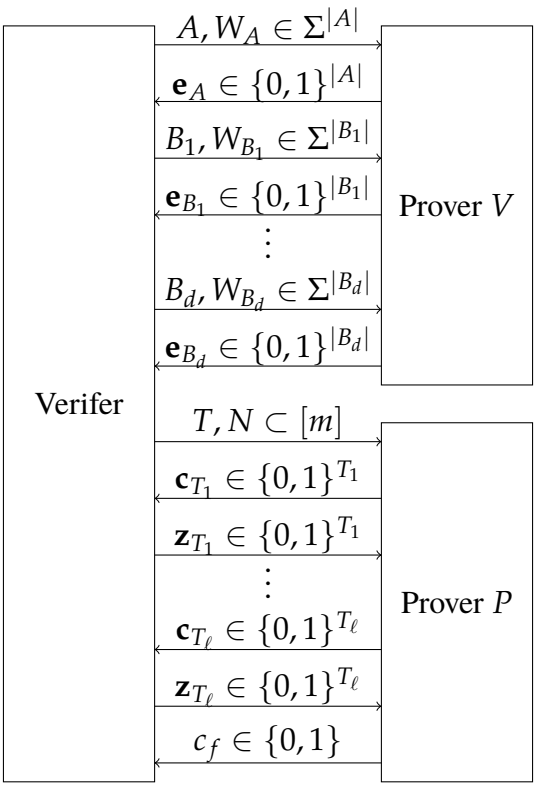


Figure 4.16: Structure of the delegation game.

From the rigidity game we may also assume that PV and PP share m EPR pairs, labeled $\{1, \ldots, m\}$, for $m = \Theta(n + t)$. We will assume that the circuit Q is broken into d layers, $Q = Q_1 \ldots Q_d$, such that in every Q_ℓ, each wire has at most one T gate applied to it, after which no other gates are applied to that wire. We will suppose the T gates are indexed from 1 to t, in order of layer.

The protocol begins with an interaction between the verifier and PV. The verifier selects a uniformly random partition $A, B_1, \ldots, B_d$ of $\{1, \ldots, m\}$, with $|A| = \Theta(n)$, and for every $\ell \in \{1, \ldots, d\}$, $|B_\ell| = \Theta(t_\ell)$, where t_ℓ is the number of T gates in Q_ℓ. The verifier also selects a uniformly random $W \in \Sigma^m$, and partitions it into substrings W_A and $W_{B_1}, \ldots, W_{B_d}$, meant to contain observables to initialize the computation qubits and auxiliary qubits for each layer of T gates respectively. The verifier instructs PV to measure his halves of the EPR pairs using the observables W_A first, and then $W_{B_1}, \ldots, W_{B_d}$, sequentially. Upon being instructed to measure a set of observables, PV measures

the corresponding half-EPR pairs and returns the results $\mathbf{e}$ to the verifier. Breaking this interaction into multiple rounds is meant to enforce that, for example, the results output by PV upon receiving W_{B_ℓ}, which we call $\mathbf{e}_{B_\ell}$, cannot depend on the choice of observables $W_{B_{\ell+1}}$. This is required for blindness.

Once the interaction with PV has been completed, as in the EPR Protocol, V selects one of three round types: computation $(r = 0)$, X-test $(r = 1)$, and Z-test $(r = 2)$. The verifier selects a subset $N \subset A$ of size n of qubits to play the role of inputs to the computation. These are chosen from the subset of A corresponding to wires that PV has measured in the appropriate observable for the round type (see Table 4.4). For example, in an X-test round, PV's EPR halves corresponding to input wires should be measured in the Z basis so that PP is left with a one-time pad of the state $|0\rangle^{\otimes n}$, so in an X-test round, the computation wires are chosen from the set $\{i \in A : W_i = Z\}$. The input wires N are labeled by $\mathcal{X}_1, \ldots, \mathcal{X}_n$.

The verifier also chooses subsets $T_\ell = T_\ell^0 \cup T_\ell^1 \subset B_\ell$ of sizes $t_{\ell,0}$ and $t_{\ell,1} = t_\ell - t_{\ell,0}$ respectively, where $t_{\ell,0}$ is the number of odd T gates in the ℓ-th layer of Q (recall the definition of even and odd T gates from Section 4.5.1.2). The wires T_ℓ^0 and T_ℓ^1 will play the role of auxiliary states used to perform T gates from the ℓ-th layer. They are chosen from those wires from B_ℓ whose corresponding EPR halves have been measured in a correct basis, depending on the round type. For example, in an X-test round, the auxiliaries corresponding to odd T gates should be prepared by measuring the corresponding EPR half in either the X or Y basis (see Table 4.3), so in an X-test round, T_ℓ^1 is chosen from $\{i \in B_\ell : W_i \in \{X, Y\}\}$ (see Table 4.4). We will let $\mathcal{T}_1, \ldots, \mathcal{T}_t$ label those EPR pairs that will be used as auxiliary states. In particular, the system $\mathcal{T}_i$ will be used for the i-th T gate in the circuit, so if the i-th T gate is even, $\mathcal{T}_i$ should be chosen from $T^0 = \cup_\ell T_\ell^0$, and otherwise it should be chosen from $T_1 = \cup_\ell T_\ell^1$. The verifier sends labels $\mathcal{T}_1, \ldots, \mathcal{T}_t$ and $\mathcal{X}_1, \ldots, \mathcal{X}_n$ to PP, who will act as P_{EPR} on the $n + t$ qubits specified by these labels.

Just as in the EPR Protocol, the input on PP's system specified by $\mathcal{X}_1, \ldots, \mathcal{X}_n$ is a quantum one-time pad of either $|\mathbf{x}\rangle$, $|0\rangle^{\otimes n}$, or $|+\rangle^{\otimes n}$, depending on the round type, with V holding the keys (determined by $\mathbf{e}$). Throughout the interaction, PP always maintains a one-time pad of the current state of the computation, with the verifier in possession of the one-time-pad keys. The verifier updates her keys as the computation is carried out, using the rules in Table 4.2.

From PP's perspective, the protocol works just as the EPR Protocol, except that he does not receive the bit z_i needed to implement the T gadget until *during* the T gadget, after he has sent V his measurement result c_i (see Figure 4.17).

To perform the i-th T gate on the j-th wire, PP performs the circuit shown in Figure 4.17. As Figure 4.17 shows, PV has already applied the observable specified by V to his half of the EPR

	Computation Round	X-test Round	Z-test Round
N, input/computation qubits	$\{i \in A : W_i = Z\}$	$\{i \in A : W_i = Z\}$	$\{i \in A : W_i = X\}$
T^0_ℓ, even T gate auxiliaries	$\{i \in B_\ell : W_i \in \{G, F\}\}$	$\{i \in B_\ell : W_i = Z\}$	$\{i \in B_\ell : W_i \in \{X, Y\}\}$
T^1_ℓ, odd T gate auxiliaries	$\{i \in B_\ell : W_i \in \{G, F\}\}$	$\{i \in B_\ell : W_i \in \{X, Y\}\}$	$\{i \in B_\ell : W_i = Z\}$

Table 4.4: How the verifier chooses index sets $T = T^0 \cup T^1$ and N for each type of round. These index sets determine which of the m systems are labeled by $\{\mathcal{T}_i\}_{i=1}^t$ and $\{\mathcal{X}_j\}_{j=1}^n$, respectively.

pair. The T gadget requires interaction with the verifier, to compute the bit z_i, which depends on the measured c_i, the value W_i, and one-time-pad key a_j, however, this interaction can be done in parallel for T gates in the same layer.

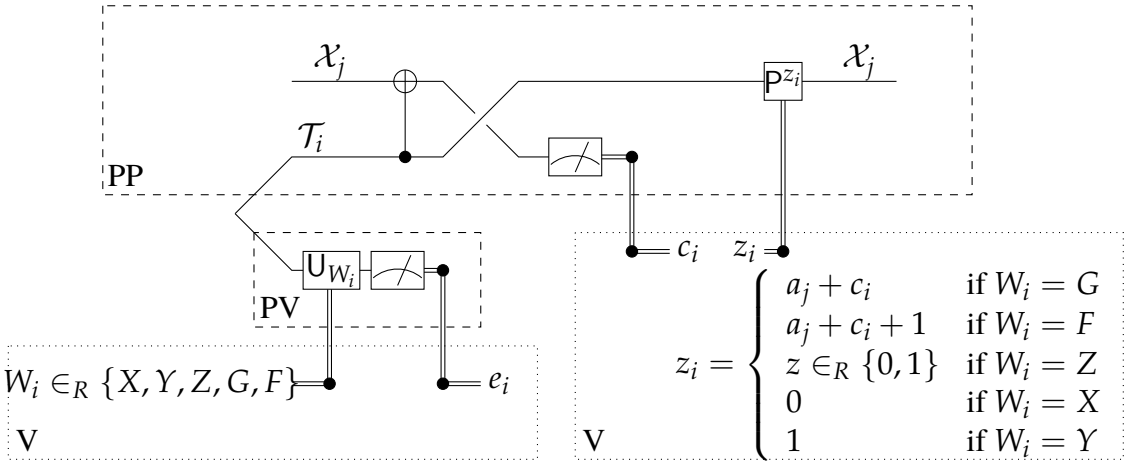


Figure 4.17: The gadget for implementing the i-th T gate, on the j-th wire.

It is simple to check that the T gadget in Figure 4.17 is the same as the T gadget for the EPR Protocol shown in Figure 4.11. In the case of the leash protocol, W is chosen at random, and then $\mathbf{z}$ is chosen accordingly, whereas in the case of the EPR Protocol, $\mathbf{z}$ is chosen at random and then W is chosen accordingly.

We now give the precise protocols for V (Figure 4.18) and honest provers PV (Figure 4.19) and PP (Figure 4.20). To see how these fit together, refer to Figure 4.16. For a string $\mathbf{v}$ and an ordered set of indices I, we denote by $\mathbf{v}_I$ the substring corresponding to indices in I.

Let $(Q, \mathbf{x})$ be the input to the verifier, where Q is compiled in the form described in Section 4.5.1.2. Let n be the size of the input to Q. Let d be the T-depth, and for $\ell \in \{1, \ldots, d\}$ let t_ℓ be the number of T gates in the ℓ-th layer.

1. The verifier selects $W \in_R \Sigma^m$. She partitions $\{1, \ldots, m\}$ arbitrarily into non-overlapping subsets A and $B_1, \ldots, B_d$ such that W_A contains at least n copies of each symbol in Σ, and for each $\ell \in \{1, \ldots, d\}$, W_{B_ℓ} contains at least t_ℓ copies of each symbol in Σ.

2. The verifier sends A, W_A to PV, who returns $\mathbf{e}_A \in \{0,1\}^A$. The verifier sequentially sends $(B_1, W_{B_1}), \ldots, (B_d, W_{B_d})$ to PV, each time receiving $\mathbf{e}_{B_\ell} \in \{0,1\}^{B_\ell}$ as answer.

3. The verifier selects a round type uniformly at random. She selects sets $N \subseteq A$ and $T_\ell \subseteq B_\ell$, for $\ell \in \{1, \ldots, d\}$, of sizes $|N| = n$ and $|T_\ell| = t_\ell$, as follows:

   Computation Round: N is chosen at random from $\{i \in A : W_i = Z\}$. T_ℓ is chosen at random from $\{i \in B_\ell : W_i \in \{G, F\}\}$. She sets $\mathbf{a} = \mathbf{e}_N + \mathbf{x}$ and $\mathbf{b} = 0^n$.

   X-test Round: N is chosen at random from $\{i \in A : W_i = Z\}$. $T_\ell = T_\ell^0 \cup T_\ell^1$, where T_ℓ^0 is of size $t_{\ell,0}$ chosen at random from $\{i \in B_\ell : W_i = Z\}$ and T_ℓ^1 is of size $t_{\ell,1}$ chosen at random from $\{i \in B_\ell : W_i \in \{X, Y\}\}$. She sets $\mathbf{a} = \mathbf{e}_N$ and $\mathbf{b} = 0^n$.

   Z-test Round: N is chosen at random from $\{i \in A : W_i = X\}$. $T_\ell = T_\ell^0 \cup T_\ell^1$, where T_ℓ^0 is of size $t_{\ell,0}$ chosen at random from $\{i \in B_\ell : W_i \in \{X, Y\}\}$ and T_ℓ^1 is of size $t_{\ell,1}$ chosen at random from $\{i \in B_\ell : W_i = Z\}$. She sets $\mathbf{a} = 0^n$ and $\mathbf{b} = \mathbf{e}_N$.

   The verifier sends the sets N and T_ℓ^0, T_ℓ^1, for all $\ell \in \{1, \ldots, d\}$, to PP.

4. For $\ell = 1, \ldots, d$,

   a) For each Clifford gate in the ℓ-th layer, perform the appropriate key update from Table 4.2.

   b) The verifier receives $\mathbf{c} = \{c_i\}_{i \in T_\ell}$ from PP. If it's an X-test round and $i \in T_\ell^0$, or it's a Z-test round and $i \in T_\ell^1$, *reject* if $c_i \neq a_j + e_i$, where j is the wire to which the i-th T gate is applied.

   c) For each $i \in T_\ell$, the verifier computes $\mathbf{z} = \{z_i\}_{i \in T_\ell}$ as follows:

   Computation Round $z_i = a_j + 1_{W_i = F} + c_i$;

   X-test Round if $i \in T_\ell^0$, $z_i \in_R \{0,1\}$; else if $i \in T_\ell^1$, $z_i = 1_{W_i = Y}$;

   Z-test Round if $i \in T_\ell^0$, $z_i = 1_{W_i = Y}$; else if $i \in T_\ell^1$, $z_i \in_R \{0,1\}$.

   d) The verifier sends $\mathbf{z}$ to PP and updates keys (a_j, b_j) for each wire j that had a T gate applied, according to Table 4.2.

5. The verifier receives a bit c_f from PP. She outputs *reject* if it's a computation or X-test round and $c_f + a_f \neq 0$, where a_f is the final X-key on the output wire; and a*ccept* otherwise.

Figure 4.18: The Delegation Game: Verifier's point of view.

1. For $\ell = 0, 1, \ldots, d$,
   a) PV receives a string $W_S \in \Sigma^S$, for some subset S of $\{1, \ldots, m\}$, from V.
   b) For $i \in S$, PV measures his half of the i-th EPR pair using the observable indicated by W_i, obtaining an outcome $e_i \in \{0, 1\}$.
   c) PV returns $\mathbf{e}_S$ to V.

Figure 4.19: The Delegation Game: Honest strategy for PV.

1. PP receives subsets N and T_ℓ^0, T_ℓ^1 of $\{1, \ldots, m\}$, for $\ell \in \{1, \ldots, d\}$, from the verifier.
2. For $\ell = 1, \ldots, d$,
   a) PP does the Clifford computations in the ℓ-th layer.
   b) For each $i \in T_\ell = T_\ell^0 \cup T_\ell^1$, PP applies a $CNOT$ from $\mathcal{T}_i$ into the input register corresponding to the wire on which this T gate should be performed, $\mathcal{X}_j$, and measures this wire to get a value c_i. The register $\mathcal{T}_i$ is relabeled $\mathcal{X}_j$. He sends $\mathbf{c}_{T_\ell} = \{c_i\}_{i \in T_\ell}$ to V. (See Figure 4.17).
   c) PP receives $\mathbf{z}_{T_\ell} = \{z_i\}_{i \in T_\ell}$ from V. For each $i \in T_\ell$, he applies P^{z_i} to the corresponding $\mathcal{X}_j$.
3. PP performs the final computations that occur after the d-th layer of T gates, measures the output qubit, $\mathcal{X}_1$, and sends the resulting bit, c_f, to V.

Figure 4.20: The Delegation Game: Honest strategy for PP.

Finally, we describe the sequential version of the game $\textsc{rigid}(\Sigma, m)$ in Figure 4.21. It is no different than $\textsc{rigid}(\Sigma, m)$, except for the fact that certain subsets of questions and answers are exchanged sequentially, but the acceptance condition is the same. As mentioned earlier, running the game sequentially only reduces the provers' ability to cheat. Hence, the guarantees from $\textsc{rigid}(\Sigma, m)$ in Section 4.4 hold verbatim for the sequential version.

Let m, n, and $t_1, \ldots, t_d$ be parameters provided as input, such that $m = \Theta(n + t_1 + \cdots + t_d)$.

1. The verifier selects questions $W, W' \in \Sigma^m$, for the first and second player respectively, according to the distribution of questions in the game $\textsc{rigid}(\Sigma, m)$. She partitions $\{1, \ldots, m\}$ at random into subsets A and B_ℓ, for $\ell \in \{1, \ldots, d\}$, of size $|A| = \Theta(n)$ and $|B_\ell| = \Theta(t_\ell)$, exactly as in Step 1 of the Delegation Game.

2. The verifier sends $(A, W_A), (B_1, W_{B_1}), .., (B_d, W_{B_d})$ and $(A, W'_A), (B_1, W'_{B_1}), .., (B_d, W'_{B_d})$ in sequence to the first and second prover respectively. They sequentially return respectively $\mathbf{e}_A \in \{0,1\}^{|A|}$, $\mathbf{e}_{B_1} \in \{0,1\}^{|B_1|}, .., \mathbf{e}_{B_d} \in \{0,1\}^{|B_d|}$ and $\mathbf{e}'_A \in \{0,1\}^{|A|}$, $\mathbf{e}'_{B_1} \in \{0,1\}^{|B_1|}, .., \mathbf{e}'_{B_d} \in \{0,1\}^{|B_d|}$.

3. The verifier accepts if and only if $\mathbf{e}, \mathbf{e}'$ and W, W' satisfy the winning condition of $\textsc{rigid}(\Sigma, m)$.

Figure 4.21: Sequential version of $\textsc{rigid}(\Sigma, m)$.

4.5.2.2 Completeness

Lemma 26. *Suppose the verifier executes the rigidity game with probability p_r and the delegation game with probability $p_d = 1 - p_r$, on an input $(Q, |\mathbf{x}\rangle)$ such that $\|\Pi_0 Q |\mathbf{x}\rangle\|^2 \geq 2/3$. Then there is a strategy for the provers which is accepted with probability at least $p_{\text{compl}} = p_r(1 - e^{-\Omega(n+t)}) + \frac{8}{9} p_d$.*

Proof. The provers PV and PP play the rigidity game according to the honest strategy, and the delegation game as described in Figures 4.19 and 4.20 respectively. Their success probability in the delegation game is the same as the honest strategy in the EPR Protocol, which is at least $\frac{2}{3} + \frac{2}{3}\frac{1}{3} = \frac{8}{9}$, by Theorem 10 and since in our protocol the verifier chooses each of the three types of rounds uniformly. □

4.5.2.3 Soundness

We divide the soundness analysis into three parts. First we analyze the case of an honest PV, and a cheating PP (Lemma 27). Then we show that if PV and PP pass the rigidity game with almost optimal probability, then one can construct new provers PV′ and PP′, with PV′ honest, such that the probability that they are accepted in the delegation game is not changed by much (Lemma 28). In Lemma 29, we combine the previous to derive the desired constant soundness-completeness gap, where we exclude that the acceptance probability of the provers in the rigidity game is too low by picking a p_r large enough.

Lemma 27 (Soundness against PP)**.** *Suppose the verifier executes the delegation game on input* $(Q, |\mathbf{x}\rangle)$ *such that* $\|\Pi_0 Q\,|\mathbf{x}\rangle\,\|^2 \leq 1/3$ *with provers* (PV, PP^*) *such that PV plays the honest strategy. Then the verifier accepts with probability at most* $7/9$*.*

Proof. Let PP* be any prover. Assume that PV behaves honestly and applies the measurements specified by his query W on halves of EPR pairs shared with PP*. As a result the corresponding half-EPR pair at PP* is projected onto the post-measurement state associated with the outcome reported by PV to V.

From PP*, we define another prover, P^*, such that if P^* interacts with V_{EPR}, the honest verifer for the EPR Protocol (Figure 4.13), then V_{EPR} rejects with the same probability that V would reject on interaction with PP*. The main idea of the proof can be seen by looking at Figure 4.17, and noticing that: (1) the combined action of V and PV is unchanged if instead of choosing the W_i-values at random and then choosing z_i as a function of these, the z_i are chosen uniformly at random, and then the W_i are chosen as a function of these; and (2) with this transformation, the combined action of V and PV is now the same as the action of V_{EPR} in the EPR Protocol.

We now define P^*. P^* acts on a system that includes $n+t$ qubits that, in an honest run of the EPR Protocol, are halves of EPR pairs shared with V_{EPR}. P^* receives $\{z_i\}_{i=1}^t$ from V_{EPR}. P^* creates $m-(n+t)$ half EPR pairs (i.e. single-qubit maximally mixed states) and randomly permutes these with his $n+t$ unmeasured qubits, n of which correspond to computation qubits on systems $\mathcal{X}_1, \ldots, \mathcal{X}_n$ — he sets N to be the indices of these qubits — and t of which correspond to T-auxiliary states — he sets T^0 and T^1 to be the indices of these qubits. P^* simulates PP* on these m qubits in the following way. First, P^* gives PP* the index sets N, T^0, and T^1. In the ℓ-th iteration of the loop (Step 2. in Figure 4.20), PP* returns some bits $\{c_i\}_{i\in T_\ell}$, and then expects inputs $\{z_i\}_{i\in T_\ell}$, which P^* provides, using the bits he received from V_{EPR}. Finally, at the end of the computation, PP* returns a bit c_f, and P^* outputs $\{c_i\}_{i\in T}$ and c_f.

This completes the description of P^*. To show the lemma we argue that for any input $(Q, |\mathbf{x}\rangle)$ the probability that V outputs a*ccept* on interaction with PV and PP* is the same as the probability that V_{EPR} outputs a*ccept* on interaction with P^*, which is at most $\frac{2}{3}q_t + \frac{1}{3}q_c$ whenever $\|\Pi_0 Q\,|\mathbf{x}\rangle\,\|^2 \leq 1/3$, by Theorem 11. Using $\delta = \frac{1}{3}$, Theorem 11 gives $q_c \leq \frac{5}{3} - \frac{4}{3}q_t$, which yields

$$\frac{2}{3}q_t + \frac{1}{3}q_c \leq \frac{5}{9} + \frac{2}{9}q_t \leq \frac{7}{9}.$$

There are two reasons that V_{EPR} might reject: (1) in a computation or X-test round, the output qubit decodes to 1; or (2) in an evaluation of the gadget in Figure 4.17 (either an X-test round for an even T gate, or a Z-test round for an odd T gate) the condition $c_i = a_j \oplus e_i$ fails.

We first consider case (1). This occurs exactly when $c_f \oplus a_f = 1$, where a_f is the final X key of the output wire, held by V_{EPR}. We note that a_f is exactly the final X key that V would hold in the Verifier-on-a-Leash Protocol, which follows from the fact that the update rules in both the EPR Protocol and the leash protocol are the same. Thus, the probability that V_{EPR} finds $v_f \oplus a_f = 1$ on interaction with P^* is exactly the probability that V finds $c_f \oplus a_f = 1$ in Step 5 of Figure 4.18.

Next, consider case (2). The condition $c_i \neq a_j \oplus e_i$ is exactly the condition in which a verifier interacting with P^* as in Figure 4.18 would reject (see Step 4.(b)).

Thus, the probability that V_{EPR} outputs r*eject* upon interaction with P^* is exactly the probability that V outputs r*eject* on interaction with PP*, which, as discussed above, is at most $7/9$. □

The following lemma shows soundness against cheating PV*.

Lemma 28. *Suppose the verifier executes the leash protocol on input $(Q, |\mathbf{x}\rangle)$ such that $\|\Pi_0 Q |\mathbf{x}\rangle\|^2 \leq 1/3$ with provers (PV^*, PP^*), such that the provers are accepted with probability $1-\varepsilon$, for some $\varepsilon > 0$, in the rigidity game, and with probability at least q in the delegation game. Then there exist provers PP' and PV' such that PV' applies the honest strategy and PP' and PV' are accepted with probability at least $q - \mathrm{poly}(\varepsilon)$ in the delegation game.*

Proof. By assumption, PP* and PV* are accepted in the rigidity game with probability at least $1-\varepsilon$. Let V_A, V_B be the local isometries guaranteed to exist by Corollary 3, and $\{\tau_\lambda\}$ the subnormalized densities associated with PP*'s Hilbert space (recall that playing the rigidity game sequentially leaves the guarantees from Corollary 3 unchanged, since it only reduces the provers' ability to cheat).

First define provers PV$''$ and PP$''$ as follows. PP$''$ and PV$''$ initially share the state

$$|\psi'\rangle_{\mathsf{AB}} = \otimes_{i=1}^{m} |\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{\mathsf{AB}} \otimes \sum_{\lambda\in\{\pm\}} |\lambda\rangle\langle\lambda|_{\mathsf{A}'} \otimes |\lambda\rangle\langle\lambda|_{\mathsf{B}'} \otimes (\tau_\lambda)_{\mathsf{A}''},$$

with registers $\mathsf{AA}'\mathsf{A}''$ in the possession of PP$''$ and BB' in the possession of PV$''$. Upon receiving a query $W \in \Sigma^m$, PV$''$ measures B' to obtain a $\lambda \in \{\pm\}$. If $\lambda = +$ he proceeds honestly, measuring his half-EPR pairs exactly as instructed. If $\lambda = -$ he proceeds honestly except that for every honest single-qubit observable specified by W, he instead measures the complex conjugate observable. Note that this strategy can be implemented irrespective of whether W is given at once, as in the game RIGID, or sequentially, as in the Delegation Game. PP$''$ simply acts like PP*, just with the isometry V_A applied.

First note that by Corollary 3, the distribution of answers of PV$''$ to the verifier, as well as the subsequent interaction between the verifier and PP, generate (classical) transcripts that are within statistical distance $\mathrm{poly}(\varepsilon)$ from those generated by PV* and PP* with the same verifier.

Next we observe that taking the complex conjugate of both provers' actions does not change their acceptance probability in the delegation game, since the interaction with the verifier is completely classical. Define PP′ as follows: PP′ measures A' to obtain the same λ as PV″, and then executes PP″ or its complex conjugate depending on the value of λ. Define PV′ to execute the honest behavior (he measures to obtain λ, but then discards it and does not take any complex conjugates).

Then PV′ applies the honest strategy, and $(\mathrm{PV}', \mathrm{PP}')$ applies either the same strategy as $(\mathrm{PV}'', \mathrm{PP}'')$ (if $\lambda = +$) or its complex conjugate (if $\lambda = -$). Therefore they are accepted in the delegation game with exactly the same probability. □

Combining Lemma 27 and Lemma 28 gives us the final soundness guarantee.

Lemma 29. *(Constant soundness-completeness gap) There exist constants $p_r, p_d = 1 - p_r$ and $\Delta > 0$ such that if the verifier executes the leash protocol with parameters (p_r, p_d) on input $(Q, |\mathbf{x}\rangle)$ such that $\|\Pi_0 Q\,|\mathbf{x}\rangle\,\|^2 \leq 1/3$, any provers (PV^*, PP^*) are accepted with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

Proof. Suppose provers PP* and PV* succeed in the delegation game with probability $\frac{7}{9} + w$ for some $w > 0$, and the testing game with probability $1 - \varepsilon_*(w)$, where $\varepsilon_*(w)$ will be specified below. By Lemma 28, this implies that there exist provers PP′ and PV′ such that PV′ is honest and the provers succeed in the delegation game with probability at least $\frac{7}{9} + w - g(\varepsilon_*(w))$, where $g(\varepsilon) = \mathrm{poly}(\varepsilon)$ is the function from the guarantee of Lemma 28. Let $\varepsilon_*(w)$ be such that $g(\varepsilon_*(w)) \leq \frac{w}{2}$. In particular, $\frac{7}{9} + w - g(\varepsilon_*(w)) \geq \frac{7}{9} + \frac{w}{2} > \frac{7}{9}$. This contradicts Lemma 27.

Thus if provers PP and PV succeed in the delegation game with probability $\frac{7}{9} + w$ they must succeed in the rigidity game with probability less than $1 - \varepsilon_*(w)$. This implies that for any strategy of the provers, on any *no* instance, the probability that they are accepted is at most

$$\max\Big\{p_r + (1-p_r)\Big(\frac{7}{9} + \frac{1}{18}\Big),\ p_r\Big(1 - \varepsilon_*\Big(\frac{1}{18}\Big)\Big) + (1-p_r)\cdot 1\Big\}.$$

Since $\varepsilon_*(\frac{1}{18})$ is a positive constant, it is clear that one can pick p_r large enough so that

$$p_r\Big(1 - \varepsilon_*\Big(\frac{1}{18}\Big)\Big) + (1-p_r)\cdot 1 < p_r + (1-p_r)\Big(\frac{7}{9} + \frac{1}{18}\Big).$$

Select the smallest such p_r. Then the probability that the two provers are accepted is at most

$$p_{\text{sound}} := p_r + (1-p_r)\Big(\frac{7}{9} + \frac{1}{18}\Big) < p_r\big(1 - e^{-\Omega(n+t)}\big) + (1-p_r)\frac{8}{9} = p_{\text{compl}},$$

which gives the desired constant completeness-soundness gap Δ. □

4.5.2.4 Blindness

We now establish blindness of the Leash Protocol. In Lemma 30, we will prove that the protocol has the property that neither prover can learn anything about the input to the circuit, $\mathbf{x}$, aside from its length. Thus, the protocol can be turned into a blind protocol, where Q is also hidden, by modifying any input $(Q, \mathbf{x})$ where Q has g gates and acts on n qubits, to an input $(U_{g,n}, (Q, \mathbf{x}))$, where $U_{g,n}$ is a universal circuit that takes as input a description of a g-gate circuit Q on n qubits, and a string $\mathbf{x}$, and outputs $Q|\mathbf{x}\rangle$. The universal circuit $U_{g,n}$ can be implemented in $O(g \log n)$ gates. By Lemma 30, running the Leash Protocol on $(U_{g,n}, (Q, \mathbf{x}))$ reveals nothing about Q or $\mathbf{x}$ aside from g and n.

In the form presented in Figure 4.18, the verifier V interacts first with PV, sending him random questions that are independent from the input $\mathbf{x}$, aside from the input length n. It is thus clear that the protocol is blind with respect to PV.

In contrast, the questions to PP depend on PV's answers and on the input, so it may a priori seem like the questions can leak information to PP. To show that the protocol is also blind with respect to PP, we show that there is an alternative formulation, in which the verifier first interacts with PP, sending him random messages, and then only with PV, with whom the interaction is now adaptive. We argue that, for an arbitrary strategy of the provers, the reduced state of all registers available to either prover, PP or PV, is exactly the same in both formulations of the protocol — the *original* and the *alternative* one. This establishes blindness for both provers. This technique for proving blindness is already used in [82] to establish blindness of a two-prover protocol based on computation by teleportation.

Lemma 30 (Blindness of the Leash Protocol)**.** *For any strategy of PV* and PP*, the reduced state of PV* (resp. PP*) at the end of the leash protocol is independent of the input* $\mathbf{x}$*, aside from its length.*

Proof. Let PV* and PP* denote two arbitrary strategies for the provers in the leash protocol. Each of these strategies can be modeled as a super-operator

$$\mathcal{T}_{\mathrm{PV}} : \mathrm{L}(\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}) \to \mathrm{L}(\mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}), \qquad \mathcal{T}_{\mathrm{PP},ad} : \mathrm{L}(\mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{PP}}) \to \mathrm{L}(\mathcal{H}_{T'_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{PP}}).$$

Here $\mathcal{H}_{T_{\mathrm{PV}}}$ and $\mathcal{H}_{T'_{\mathrm{PV}}}$ (resp. $\mathcal{H}_{T_{\mathrm{PP}}}$ and $\mathcal{H}_{T'_{\mathrm{PP}}}$) are classical registers containing the inputs and outputs to and from PV* (resp. PP*), and $\mathcal{H}_{\mathrm{PV}}$ (resp. $\mathcal{H}_{\mathrm{PP}}$) is the private space of PV* (resp. PP*). Note that the interaction of each prover with the verifier is sequential, and we use $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$ to denote the combined action of the prover and the verifier across all rounds of interaction (formally these are sequences of superoperators).

Consider an alternative protocol, which proceeds as follows. The verifier first interacts with PP. From Figure 4.20 we see that the inputs required for PP are subsets N and $T_1, \ldots, T_d$, and values $\{z_i\}_{i \in T_\ell}$ for each $\ell \in \{1, \ldots, d\}$. To select the former, the verifier proceeds as in the first step of the Delegation Game. She selects the latter uniformly at random. The verifier collects values $\{c_i\}_{i \in T_\ell}$ from PP exactly as in the original Delegation Game.

Once the interaction with PP has been completed, the verifier interacts with PV. First, she selects a random string $W_N \in \Sigma^N$, conditioned on the event that W_N contains at least n copies of each symbol in Σ, and sends it to PV, collecting answers $\mathbf{e}_N$. The verifier then follows the same update rules as in the delegation game. We describe this explicitly for computation rounds. First, the verifier sets $\mathbf{a} = \mathbf{e}_N$. Depending on the values $\{c_i\}_{i \in T_1}$ and $\{z_i\}_{i \in T_1}$ obtained in the interaction with PP, using the equation $z_i = a_j + 1_{W_i = F} + c_i$ she deduces a value for $1_{W_i = F}$ for each $i \in T_1 \subseteq B_1$. She then selects a uniformly random $W_{B_1} \in \Sigma^{B_1}$, conditioned on the event that W_{B_1} contains at least t_1 copies of each symbol from Σ, and for $i \in T_1$ it holds that $W_i = F$ if and only if $z_i = a_j + 1 + c_i$. The important observation is that, if T_1 is a uniformly random, unknown subset, the marginal distribution on W_{B_1} induced by the distribution described above is independent of whether $z_i = a_j + 1 + c_i$ or $z_i = a_j + 0 + c_i$: precisely, it is uniform conditioned on the event that W_{B_1} contains at least t_1 copies of each symbol from Σ. The verifier receives outcomes $\mathbf{e}_{B_1} \in \{0,1\}^{B_1}$ from PV, and using these outcomes performs the appropriate key update rules; she then proceeds to the second layer of the circuit, until the end of the computation. Finally, the verifier accepts using the same rule as in the last step of the original delegation game.

We claim that both the original and alternative protocols generate the same joint final state:

$$\mathcal{T}_{\mathrm{PP},ad} \circ \mathcal{T}_{\mathrm{PV}}(\rho_{orig}) \;=\; \mathcal{T}_{\mathrm{PV},ad} \circ \mathcal{T}_{\mathrm{PP}}(\rho_{alt}) \;\in\; \mathcal{H}_{\mathrm{PP}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{V}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}, \qquad (4.26)$$

where we use ρ_{orig} and ρ_{alt} to denote the joint initial state of the provers, as well as the verifier's initialization of her workspace, in the original and alternative protocols respectively, and $\mathcal{T}_{\mathrm{PV},ad}$ and $\mathcal{T}_{\mathrm{PP}}$ are the equivalent of $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$ for the reversed protocol (in particular they correspond to the same strategies PV^* and PP^* used to define $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$). Notice that $\mathcal{T}_{\mathrm{PV},ad}$ and $\mathcal{T}_{\mathrm{PP}}$ are well-defined since neither prover can distinguish an execution of the original from the alternative protocol.[8] To see that equality holds in (4.26), it is possible to re-write the final state of the protocol as the result of the following sequence of operations. First, the verifier initializes the message registers with PP^* and PV^* using half-EPR pairs, keeping the other halves in her private workspace. This simulates the generation of uniform random messages to both provers. Then, the superoperator $\mathcal{T}_{\mathrm{PV}} \otimes \mathcal{T}_{\mathrm{PP}}$ is executed. Finally, the verifier post-selects by applying a projection

[8] One must ensure that a prover does not realize if the alternative protocol is executed instead of the original; this is easily enforced by only interacting with any of the provers at specific, publicly decided times.

operator on $\mathcal{H}_{T_{\text{PV}}} \otimes \mathcal{H}_{T'_{\text{PV}}} \otimes \mathcal{H}_{T_{\text{PP}}} \otimes \mathcal{H}_{T'_{\text{PP}}}$ that projects onto valid transcripts for the original protocol (i.e. transcripts in which the adaptive questions are chosen correctly). This projection can be implemented in two equivalent ways: either the verifier first measures $\mathcal{H}_{T_{\text{PV}}} \otimes \mathcal{H}_{T'_{\text{PV}}}$, and then $\mathcal{H}_{T_{\text{PP}}} \otimes \mathcal{H}_{T'_{\text{PP}}}$; based on the outcomes she accepts a valid transcript for the original protocol or she rejects. Or, she first measures $\mathcal{H}_{T_{\text{PP}}} \otimes \mathcal{H}_{T'_{\text{PP}}}$, and then $\mathcal{H}_{T_{\text{PV}}} \otimes \mathcal{H}_{T'_{\text{PV}}}$; based on the outcomes she accepts a valid transcript for the alternative protocol or she rejects. Using the commutation of the provers' actions, conditioned on the transcript being accepted, the first gives rise to the first final state in (4.26), and the second to the second final state. The two are equivalent because the acceptance condition for a valid transcript is identical in the two versions of the protocol.

Since in the first case the reduced state on $\mathcal{H}_{T'_{\text{PV}}} \otimes \mathcal{H}_{\text{PV}}$ is independent of the input to the computation, $\mathbf{x}$, and in the second the reduced state on $\mathcal{H}_{\text{PP}} \otimes \mathcal{H}_{T'_{\text{PP}}}$ is independent of $\mathbf{x}$, we deduce that the protocol hides the input from each of PV* and PP*. □

4.5.3 The Dog-Walker Protocol

4.5.3.1 Protocol and statement of results

The Dog-Walker Protocol again involves a classical verifier V and two provers PV and PP. As in the leash protocol presented in Section 4.5.2, PP and PV take the roles of P_{EPR} and V_{EPR} from [11] respectively. The main difference is that the Dog-Walker Protocol gives up blindness in order to reduce the number of rounds to two (one round of interaction with each prover, played sequentially). After one round of communication with PP, who returns a sequence of measurement outcomes, V communicates all of PP's outcomes, except for the one corresponding to the output bit of the computation, as well as the input $\mathbf{x}$, to PV. With these, PV can perform the required adaptive measurements without the need to interact with V. It may seem risky to communicate bits sent by PP directly to PV — this seems to allow for communication between the two provers! Indeed, blindness is lost. However, if PP is honest, his outcomes $\{c_i\}_i$ in the computation round are the result of measurements he performs on half-EPR pairs, and are uniform random bits. If he is dishonest, and does not return the outcomes obtained by performing the right measurements, he will be caught in the test rounds. It is only in computation rounds that V sends the measurement results $\{c_i\}_i$ to PV.

To guarantee that PV behaves honestly, we combine the rigidity test $\textsc{rigid}(\Sigma, m)$ from Section 4.4.4 with the tomography test $\textsc{tom}(\Sigma, n+t, m)$ from Section 4.4.5. Part of the latter test requires PV to announce what measurements he has performed and the corresponding outcomes he obtained. He has to do so honestly in order to pass the test.

Throughout this section we let $\Sigma = \{X, Y, Z, F, G\}$, and let $m = \Theta(n+t)$ be chosen large enough so that each symbol in Σ appears at least $n+t$ times in a uniform random $W \in \Sigma^m$, with

probability close to 1. Let $\mu(W)$ denote the probability that a player receives input W while playing $\textsc{rigid}(\Sigma, m)$ (recall that both players have the same marginals in $\textsc{rigid}$). Let $\mu(W'|W)$ denote the probability that one player receives W' given that the other player receives W.

The full protocols are presented in Figure 4.22 (verifier's point of view), Figure 4.24 (PV's point of view) and Figure 4.23 (PP's point of view). The protocol has two types of rounds: EPR and Rigidity. Within an EPR round are three types of sub-rounds: Computation sub-round, X-test sub-round, and Z-test sub-round. We will generally think of X- and Z-test sub-rounds as one sub-round type (Test sub-round). Within a Rigidity round are two types of sub-rounds: Tomography sub-round, which should be thought of as the Rigidity version of the EPR-Computation round; and Clifford sub-round, which should be thought of as the Rigidity version of the EPR-Test round. With some probability p_1, V runs a Rigidity round, Clifford sub-round; with some probability p_2, V runs an EPR round, Test sub-round; with some probability p_3, V runs an EPR round, Computation sub-round; and with probability $p_4 = 1 - p_1 - p_2 - p_3$, V runs a Rigidity round, Tomography sub-round. We call this the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4).

The following theorem states the guarantees of the Dog-Walker Protocol.

Theorem 13. *There exist constants p_1, p_2, p_3, $p_4 = 1 - p_1 - p_2 - p_3$, and $\Delta > 0$ such that the following hold of the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4), when executed on input $(Q, |\mathbf{x}\rangle)$.*

- *(Completeness:) Suppose that $\|\Pi_0 Q\,|\mathbf{x}\rangle\|^2 \geq 2/3$. Then there is a strategy for PV and PP that is accepted with probability at least $p_{\text{compl}} = p_1(1 - e^{-\Omega(n+t)}) + p_2 + \frac{2}{3}p_3 + p_4$.*
- *(Soundness:) Suppose that $\|\Pi_0 Q\,|\mathbf{x}\rangle\|^2 \leq 1/3$. Then any strategy for PV and PP is accepted with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

The proof of completeness is given in Lemma 31, and proof of soundness is given in Lemma 36.

1. Select a round type **EPR** or **Rigidity**, and disjoint sets $N, T^0, T^1 \subset \{1, \ldots, m\}$ of sizes n, t_0 and $t - t_0$.

EPR Choose $\mathbf{z}$ uniformly at random from $\{0,1\}^t$ and send it, along with N, T^0 and T^1, to PP. Receive measurement outcomes $\mathbf{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ from PP.

Rigidity Choose W' according to $\mu(\cdot)$ and send it to PP. Receive $\mathbf{e}' \in \{0,1\}^m$ from PP.

2. Select a sub-round type at random from **Computation**, **X Test** or **Z Test**.

Computation Based on whether it's an EPR or a Rigidity Round:

EPR (i) Send $\mathbf{x}$, $\mathbf{z}$, $\mathbf{c}$ and sets N, T^0 and T^1 to PV, and receive measurement outcomes $\mathbf{a}, \mathbf{b} \in \{0,1\}^n$ and $\mathbf{e} \in \{0,1\}^t$.

(ii) Apply the update rules from Table 4.2 gate-by-gate to obtain the final X key for the output wire a'_f. If $c_f + a'_f \neq 0$, *reject*.

Rigidity (Tomography) (i) Choose uniform random strings $\mathbf{c}, \mathbf{z} \in \{0,1\}^t$, $\mathbf{x} \in \{0,1\}^n$ to send to PV, along with N and T, and receive measurement outcomes $\mathbf{d} \in \{0,1\}^n$ and $\mathbf{e} \in \{0,1\}^t$.

(ii) From $\mathbf{x}$, $\mathbf{c}$, $\mathbf{z}$, $\mathbf{d}$, and $\mathbf{e}$, determine the adaptive measurements $W \in \Sigma^{n+t}$ that V^0_{EPR} would have performed (based on Figure 4.14), and *reject* if the input-output pairs $(W', \mathbf{e}')$ and $(N \cup T, (W, \mathbf{e}))$ do not satisfy the winning criterion for $\textsc{tom}(\Sigma, n + t, m)$.

X**-Test** Based on whether it's an EPR or a Rigidity Round:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = Z$ for all $i \in N$; $W_i = Z$ for all $i \in T^0$; and $W_i \in \{X, Y\}$ for all $i \in T^1$. Send W to PV and receive measurement results $\mathbf{e} \in \{0,1\}^m$. Let $(\mathbf{a}, \mathbf{b}) = (\mathbf{e}_N, 0^n)$.

(ii) Apply update rules from Table 4.2 gate-by-gate to obtain $\forall i \in [t]$ the X key before the i-th T gate is applied, a'_i, and the final X key for the output wire, a'_f. If $\exists i$ s.t. the i-th T gate is even and $c_i \neq a'_i + e_i$, *reject*. If $c_f + a'_f \neq 0$, *reject*.

Rigidity (Clifford) Choose W according to the marginal conditioned on W', $\mu(\cdot|W')$. Send W to PV and receive $\mathbf{e} \in \{0,1\}^m$. Reject if $(W', \mathbf{e}', W, \mathbf{e})$ doesn't win $\textsc{rigid}(\Sigma, m)$.

Z**-Test** Based on whether it's an EPR or a Rigidity Round:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = X$ for all $i \in N$; $W_i \in \{X, Y\}$ for all $i \in T^0$; and $W_i = Z$ for all $i \in T^1$. Send W to PV and receive measurement results $\mathbf{e} \in \{0,1\}^m$. Let $(\mathbf{a}, \mathbf{b}) = (0^n, \mathbf{e}_N)$.

(ii) Apply update rules from Table 4.2 gate-by-gate to obtain $\forall i \in [t]$, the X key before the i-th T gate is applied, a'_i. If $\exists i$ s.t. the i-th T gate is odd and $c_i \neq a'_i + e_i$, *reject*.

Rigidity (Clifford) Identical to X-Test case.

Figure 4.22: The Dog-Walker Protocol: Verifier's point of view.

1. If PP receives a question W' from V (he is playing TOM or RIGID):

   Measure the m qubits in the observable indicated by W' — for example, if $W' \in \Sigma^m$, for $i \in \{1, \ldots, m\}$, measure the i-th qubit in the basis indicated by W'_i — and report the outcomes $\mathbf{e}'$ to V.

2. If PP receives $\mathbf{z}$, and sets N, T^0 and T^1 from V (he is playing the role of P_{EPR} from the EPR Protocol):

   Run the prover P_{EPR} from Figure 4.15 on input $\mathbf{z}$, the n qubits in N, and the t qubits in $T^0 \cup T^1$. Report the outputs $\mathbf{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ of P_{EPR} to V.

Figure 4.23: The Dog-Walker Protocol: Honest strategy for PP.

1. If PV receives a question W from V (he is playing RIGID or an X- or Z-Test Round):

   Measure the m qubits in the observable indicated by W — for example, if $W \in \Sigma^m$, for $i \in \{1, \ldots, m\}$, measure the i-th qubit in the basis indicated by W_i — and report the outcomes $\mathbf{e}$ to V.

2. If PV receives $\mathbf{x}$, $\mathbf{z}$, $\mathbf{c}$ and sets N, T^0 and T^1 from V (he is playing TOM or a Computation Round):

   Run the procedure V^0_{EPR} from Figure 4.14 on input $\mathbf{x}$, $\mathbf{c}$, $\mathbf{z}$, the n qubits in N, and the t qubits in $T^0 \cup T^1$. Report the outputs $\mathbf{d}$ and $\mathbf{e}$ of V^0_{EPR} to V.

Figure 4.24: The Dog-Walker Protocol: Honest strategy for PV.

4.5.3.2 Completeness

Lemma 31. *Suppose V executes the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4). There is a strategy for the provers such that, on any input $(Q, |\mathbf{x}\rangle)$ such that $\|\Pi_0 Q |\mathbf{x}\rangle\|^2 \geq \frac{2}{3}$, V accepts with probability at least $p_{\text{compl}} = p_1(1-\delta_c) + p_2 + \frac{2}{3}p_3 + p_4$, for some $\delta_c = e^{-\Omega(n+t)}$.*

Proof. The provers PV and PP play the strategy described in Figures 4.24 and 4.23 respectively. In the Rigidity-Tomography round, the verification performed by V amounts to playing $\text{TOM}(\Sigma, n+t, m)$ with the provers (with an extra constraint on the output W of PV that is always satisfied by the honest strategy). This game has perfect completeness, which makes the V accept with probability 1 in the Rigidity-Tomography round. In the Rigidity-Clifford round, V plays $\text{RIGID}(\Sigma, m)$ with the provers. The game has completeness at least $1-\delta_c$ for some $\delta_c = e^{-\Omega(n+t)}$, since $m = \Omega(n+t)$, and therefore their success probability in this round is at least $1-\delta_c$.

In the EPR round, the provers are exactly carrying out the EPR Protocol, with V using PV to run V^r_{EPR}, and PP playing the role of P_{EPR}. Thus, test rounds result in acceptance with probability 1, and the computation round results in acceptance with probability $\|\Pi_0 Q |\mathbf{x}\rangle\|^2$, by Theorem 10. □

4.5.3.3 Soundness

Figure 4.25 summarizes the high-level structure of the soundness analysis. Intuitively, our ultimate goal is to argue that both provers either apply the correct operations in EPR-Computation rounds, or are rejected with constant probability. This will be achieved by employing a form of "hybrid argument" whereby it is argued that the provers, if they are not caught, must be using the honest strategies described in Figure 4.23 and Figure 4.24 in the different types of rounds considered in the protocol. Towards this, we divide the round types into the following four scenarios:

1. Rigidity-Clifford: The round type is **Rigidity** and the sub-round type is either X**-Test** or Z**-Test**. (When the provers are honest) PV behaves as in Item 1 of Figure 4.24, and PP behaves as in Item 1 of Figure 4.23.

2. EPR-Test: The round type is **EPR** and the sub-round type is either X**-Test** or Z**-Test**. PV behaves as in Item 1 of Figure 4.24, and PP behaves as in Item 2 of Figure 4.23.

3. EPR-Computation: The round type is **EPR** and the sub-round type is **Computation**. PV behaves as in Item 2 of Figure 4.24, and PP behaves as in Item 2 of Figure 4.23.

4. Rigidity-Tomography: The round type is **Rigidity** and the sub-round type is **Computation**. PV behaves as in Item 2 of Figure 4.24, and PP behaves as in Item 1 of Figure 4.23.

Examining Figure 4.22, we can see the following. In the Rigidity-Clifford scenario, the verifier is precisely playing the game RIGID with the provers, as the provers receive questions W' and W distributed according to $\mu(\cdot,\cdot)$, the distribution of questions for RIGID(Σ, m); their answers are tested against the winning conditions of RIGID(Σ, m). In the Rigidity-Tomography scenario, the verifier plays a variant of the game TOM with the provers, in which PV's choice of observable W is uniquely determined by his inputs $\mathbf{x}$, $\mathbf{c}$ and $\mathbf{z}$: it should match the observable implemented by V^0_{EPR} on these inputs. In EPR rounds, PV plays the part of V^r_{EPR} from the EPR Protocol, and PP play the part of P_{EPR}. The EPR-Test scenario corresponds to X- and Z-tests from the EPR Protocol, whereas the EPR-Computation scenario corresponds to computation rounds from the EPR Protocol.

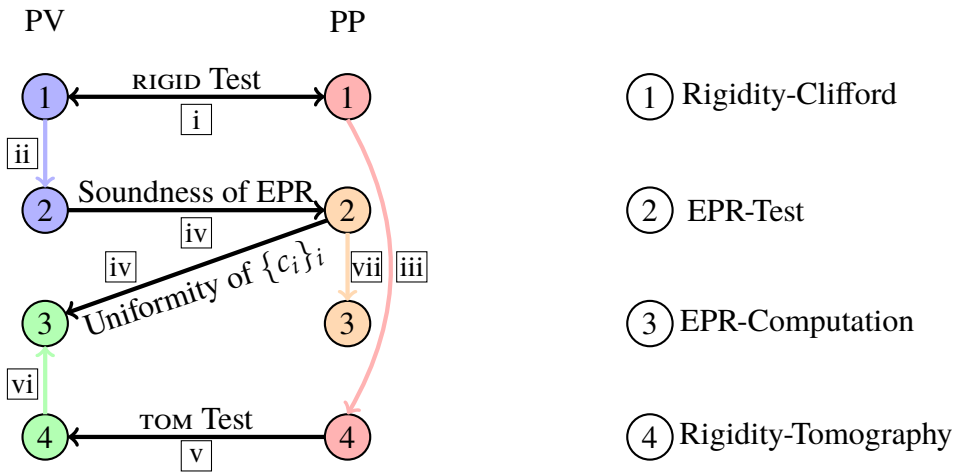


Figure 4.25: Overview of the soundness of the Dog-Walker Protocol

The structure of the proof is as follows (see also Figure 4.25):

(i) By the game RIGID, in the Rigidity-Clifford rounds, both PP and PV must be honest, or they would lose the game.

(ii) Since PV can't distinguish between Rigidity-Clifford and EPR-Test (both are Figure 4.24 Item 1 from his perspective, and the input distributions, while not identical, are within constant total variation distance), PV must be honest in the EPR-Test rounds, by (i).

(iii) Since PP can't distinguish between Rigidity-Clifford and Rigidity-Tomography (both are Figure 4.23 Item 1 from his perspective), PP must be honest in the Rigidity-Tomography rounds, by (i).

(iv) Since PV is honest in EPR-Test rounds by (ii), PP must be honest in EPR-Test rounds or he will get caught, but in particular, he must output values $\{c_i\}_{i\in[t]}$ that are uniform random and independent of $\mathbf{z}$. Since PP can't distinguish between EPR-Test and EPR-Computation rounds, this is also true in EPR-Computation rounds, when the verifier sends the values $\{c_i\}_i$ to PV.

(v) PV must be honest in Rigidity-Tomography rounds, or the provers would lose the game TOM.

(vi) Since PV can't distinguish between Rigidity-Tomography rounds and EPR-Computation rounds (both are Figure 4.24 Item 2 from his perspective), PV must be honest in EPR-Computation rounds, by (v), and his input distribution to both rounds is within constant total variation distance, by (iv).

(vii) Since PV is honest in EPR-Test rounds by (ii), and EPR-Computation rounds by (vi), the combined behavior of V and PV in the EPR rounds is that of V_{EPR} in the EPR Protocol, so by the soundness of the EPR Protocol, PP must be honest in EPR-Computation rounds, or get caught in the EPR-Test rounds with high probability.

The following lemma establishes (i), (ii) and (iii).

Lemma 32. *Suppose the verifier executes the Dog-Walker Protocol with provers (PV^*, PP^*) such that the provers are accepted with probability $q_1 \geq 1 - \varepsilon$ in the Rigidity-Clifford Round, q_2 in the EPR-Test Round, q_3 in the EPR-Computation Round, and q_4 in the Rigidity-Tomography Round. Then there exist provers (PV', PP') such that:*

- *PV' and PP' both apply the honest strategy in the Rigidity-Clifford rounds, PV' applies the honest strategy in the EPR-Test rounds, and PP' applies the honest strategy in the Rigidity-Tomography rounds; in particular, the state shared by the provers at the beginning of the protocol is a tensor product of the honest state consisting of m shared EPR pairs and an arbitrary shared ancilla;*
- *The provers are accepted with probability $q_2' = q_2 - O(\mathrm{poly}(\varepsilon))$ in the EPR-Test Round, $q_3' = q_3$ in the EPR-Computation Round, and $q_4' = q_4 - O(\mathrm{poly}(\varepsilon))$ in the Rigidity-Tomography Round.*

Proof. Using a similar argument as in Lemma 28, the strategy of PV* in Rigidity-Clifford rounds, which is also his strategy in EPR-Test rounds (Figure 4.24 Item 1); and the strategy of PP* in Rigidity-Clifford rounds, which is also his strategy in Rigidity-Tomography rounds (Figure 4.23 Item 1); can both be replaced with the honest strategies. Since the distribution of inputs to PP* in the Rigidity-Tomography rounds and Rigidity-Clifford rounds is the same, the success probability in the Rigidity-Tomography rounds is changed by at most $O(\mathrm{poly}(\varepsilon))$ by using the honest strategy. On the other hand, PV*'s input distribution in EPR-Test rounds is uniform on Σ^m, whereas his distribution in Rigidity-Clifford rounds is given by μ. However, from the description of the test RIGID it is clear that for all $W \in \Sigma^m$, $\mu(W) \geq \frac{1}{c|\Sigma|^m}$ for some constant $c > 1$, thus the total variation distance between the two distributions is at most $1 - \frac{1}{c}$. Thus, replacing PV* with the honest strategy in the EPR-Test rounds will change the success probability by at most $O(\mathrm{poly}(\varepsilon))$.

Finally, since the provers' strategy in the EPR-Computation round has not changed, the acceptance probability in it remains unchanged. □

Next, we will show that whenever PV* is honest in the EPR-Test rounds this forces PP* to output (close to) uniformly random $\{c_i\}_{i\in[t]}$ that are independent of the round type, even given $\mathbf{z}$. This

will allow us to verify that PP* is unable to signal to PV* whether the round is an EPR Round in the EPR-Computation round, when PV* is sent $\mathbf{z}$ and $\mathbf{c}$. This establishes (iv).

Lemma 33. *Suppose the verifier executes the Dog-Walker Protocol with provers (PV^*, PP^*) such that the initial shared state of the provers consists of m shared EPR pairs, together with an arbitrary shared auxiliary state; PV* plays the honest strategy in the EPR-Test rounds; the provers are accepted with probability q_1 in the Rigidity-Clifford Round, $q_2 = 1 - \varepsilon'$ in the EPR-Test Round, q_3 in the EPR-Computation Round, and q_4 in the Rigidity-Tomography Round. Then the input $(\mathbf{c}, \mathbf{z})$ given by the verifier to PV* in the EPR-Computation rounds has a distribution that is within $O(\varepsilon')$ total variation distance of uniform on $\{0,1\}^t \times \{0,1\}^t$.*

Proof. Let a'_i denote the X key of the wire to which the i-th T gate is applied, just before the i-th T gate is applied, and let D_i be a random variable defined as follows. If the i-th T gate is even, let $D_i = e_i + a'_i$, where we interpret e_i and a'_i as the random variables representing the measurement result and key V would get if she chooses to execute an X-Test round. If the i-th T gate is odd, let $D_i = e_i + a'_i$, where we interpret e_i and a'_i as the measurement result and key V would get if she chooses to execute an Z-Test round. Since PV* is assumed to play honestly in EPR-Test rounds, $\mathbf{D}$ is uniformly distributed in $\{0,1\}^t$. In particular, we have, for any $\mathbf{d}, \mathbf{z} \in \{0,1\}^t$,

$$\Pr[\mathbf{D} = \mathbf{d}, \mathbf{Z} = \mathbf{z}] = \frac{1}{4^t}.$$

Let C_i be the random variable that corresponds to the measurement output of the i-th T gadget by PP* in X-Test round if the i-th T gate is even, or the measurement output of the i-th T gadget by PP* in Z-Test round if the i-th T gate is odd.

Let $T^0 \subset [t]$ be the set of even T gates and $T^1 \subset [t]$ the set of odd T gates. In an X-Test Round, the provers are rejected whenever $i \in T^0$ and $c_i \neq d_i$, and in a Z-Test Round, they are rejected whenever $i \in T^1$ and $c_i \neq d_i$. An EPR-Test Round consists of running one of these two rounds with equal probability, so:

$$\Pr[\mathbf{C} \neq \mathbf{D}] \leq 2\varepsilon'. \tag{4.27}$$

We can express (4.27) as

$$\Pr[(\mathbf{C}, \mathbf{Z}) \neq (\mathbf{D}, \mathbf{Z})] \leq 2\varepsilon'.$$

We conclude by using the easily verifiable fact that for any random variables X and Y such that $\Pr[X = Y] \geq 1 - 2\varepsilon'$, the total variation distance between the marginal distributions on X and Y is at most $2\varepsilon'$. □

Next, we can use the tomography test TOM to establish (v), and then the fact that by Lemma 33 the input to PV is not very different in EPR-Computation and Rigidity-Tomography rounds to establish (vi):

Lemma 34. *Suppose the verifier executes the Dog-Walker Protocol with provers (PV^*, PP^*) such that: PV^* applies the honest strategy in EPR-Test rounds; PP^* applies the honest strategy in the Rigidity-Tomography rounds; and the provers are accepted with probability q_1 in the Rigidity-Clifford Round, $q_2 = 1-\varepsilon'$ in the EPR-Test Round, q_3 in the EPR-Computation Round, and $q_4 = 1-\varepsilon$ in the Rigidity-Tomography Round. Then there exist provers (PV', PP') such that PV' applies the honest strategy in the Rigidity-Tomography rounds and EPR-Computation rounds, PP' applies the honest strategy in Rigidity-Tomography rounds, and the provers are accepted with probability q_1 in the Rigidity-Clifford Round, $q_2 = 1-\varepsilon'$ in the EPR-Test Round and $q_3 - \mathrm{poly}(\varepsilon) - O(\varepsilon')$ in the EPR-Computation round.*

Proof. The Rigidity-Tomography rounds can be seen as V playing the Tomography Game with the provers, except that whereas PV* gets no non-trivial input in the Tomography Game, in the Rigidity-Tomography round, he gets random values $\mathbf{c}$ and $\mathbf{z}$ on which his strategy can depend. Fix $\mathbf{x}$, and let $\{Q^u_{\mathbf{c},\mathbf{z}}\}_u$ be the projective measurement that PV* applies upon receiving $\mathbf{c}, \mathbf{z}, \mathbf{x}$, where $u = (\mathbf{d}, \mathbf{e})$ is the string of outcomes obtained by PV on the $n+t$ single-qubit measurements he is to perform according to Step 2 in Figure 4.24.

By Corollary 4, since the provers win the Rigidity-Tomography round with probability $1-\varepsilon$, for every $\mathbf{c}, \mathbf{z} \in \{0,1\}^t$, there exist distributions $q_{\mathbf{c},\mathbf{z}}$ on $\Sigma^m \times \{\pm\}$ such that the following is $O(\mathrm{poly}(\varepsilon))$:

$$\mathbb{E}_{\mathbf{c},\mathbf{z}} \sum_{u\in\{0,1\}^m} \left\| \mathrm{Tr}_{\mathsf{A},\hat{\mathsf{B}}} \left((\mathbb{1}_{\mathsf{A}} \otimes V_{\mathsf{B}} Q^u_{\mathbf{c},\mathbf{z}}) \left|\psi\right\rangle \left\langle\psi\right|_{\mathsf{AB}} (\mathbb{1}_{\mathsf{A}} \otimes V_{\mathsf{B}} Q^u_{\mathbf{c},\mathbf{z}})^\dagger \right) - \sum_{\lambda\in\{\pm\}} q_{\mathbf{c},\mathbf{z}}(W',\lambda) \left(\bigotimes_{i=1}^m \frac{\sigma^{u_i}_{W'_i,\lambda}}{2} \right) \right\|_1 . \tag{4.28}$$

Here we use the notation from Corollary 3 and 4. The string $W' = W(\mathbf{c}, \mathbf{z}, \mathbf{u}) \in \Sigma^m$ is uniquely determined by $\mathbf{c}, \mathbf{z}$, and the outcomes u reported by PV*; indeed it is using this string that PV*'s answers are checked against the measurement outcomes obtained by PP*, who by assumption applies the honest strategy. For any fixed (W', λ) the distribution on outcomes u obtained in the "honest" strategy represented by the right-hand side in (4.28) is uniform. Thus the outcomes u reported by PV* are within $\mathrm{poly}(\varepsilon)$ of uniform. From this it follows that the joint distribution on transcripts $(\mathbf{c}, \mathbf{z}, u, W' = W(\mathbf{c}, \mathbf{z}, u))$ that results from an interaction with PV* is within statistical distance $\mathrm{poly}(\varepsilon)$ of the distribution generated by an interaction with the honest PV; furthermore, by (4.28) the resulting post-measurement states on PP* are also $\mathrm{poly}(\varepsilon)$ close to the honest ones, on average over this distribution.

We can now consider two provers PV′ and PP′ who, in Rigidity-Tomography rounds, first apply the isometries V_A, V_B from Corollary 4, then measure their auxiliary systems $\hat{\mathsf{A}}$ and $\hat{\mathsf{B}}$ using Δ_Y, obtaining a shared outcome $\lambda \in \{\pm\}$, and finally apply the honest strategy shown in Item 2 of Figure 4.24 ($\lambda = +$) or its conjugate ($\lambda = -$). Furthermore, conjugating the honest strategy produces exactly the same statistics as the honest strategy itself, so we may in fact assume that PV′ and PP′ both apply the honest strategy in Rigidity-Tomography rounds.

A consequence of PV′ applying the honest strategy in Figure 4.24 Item 2 is that PV′ also plays the honest strategy in EPR-Computation rounds. Since PV′ is still honest in the EPR-Test round and $q_2 = 1 - \varepsilon'$, Lemma 33 implies that the distribution of the input to PV′ in EPR-Computation rounds is within $\mathrm{poly}(\varepsilon) + O(\varepsilon')$ total variation distance of his input in Rigidity-Tomography rounds, therefore the provers' success probability in EPR-Computation rounds changes at most by $\mathrm{poly}(\varepsilon) + O(\varepsilon')$. □

Finally, we show that if PV is honest, then PP must be honest in EPR computation rounds, or the acceptance probability would be low, establishing (vii):

Lemma 35. *Suppose V executes the Dog-Walker Protocol on an input $(Q, |\mathbf{x}\rangle)$ such that $\|\Pi_0 Q |\mathbf{x}\rangle\|^2 \leq 1/3$, with provers (PV, PP) such that PV plays the honest strategy. Let q_2 be the provers' acceptance probability in EPR-Test rounds. Then the verifier accepts with probability at most $p_1(1 - \delta_c) + p_2 q_2 + p_3(5/3 - 4q_2/3) + p_4$.*

Proof. With probability $p_2 + p_3$, V executes an EPR round, in which case, he executes EPR-Computation with probability $\frac{p_3}{p_2+p_3}$ and EPR-Test with probability $\frac{p_2}{p_2+p_3}$. In the former case, since PV is honest, he is executing V^0_{EPR}. In fact, the behavior of an honest PV in the EPR-Test rounds is also that of V^r_{EPR}. Thus, the combined behavior of V and PV is that of V_{EPR}. Then the result follows from Theorem 11. □

We can now combine Lemmas 32, 34, and 35 to get the main result of this section, the "soundness" part of Theorem 13.

Lemma 36 (Constant soundness-completeness gap)**.** *There exist constants p_1, p_2, p_3, $p_4 = 1 - p_1 - p_2 - p_3$ and $\Delta > 0$ such that if the verifier executes the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4) on input $(Q, |\mathbf{x}\rangle)$ such that $\|\Pi_0 Q |\mathbf{x}\rangle\|^2 \leq 1/3$, then any provers (PV^*, PP^*) are accepted with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

Proof. Suppose the provers PV* and PP* are such that the lowest acceptance probability in either the Rigidity-Clifford round or the Rigidity-Tomography round is $1 - \varepsilon$, and they are accepted with

probability $1-\varepsilon'$ in the EPR-Test round, and with probability $1/3+w$ in the Computation Round. Applying Lemma 32 and Lemma 34 in sequence, we deduce the existence of provers $(\mathrm{PV}', \mathrm{PP}')$ for which

$$\begin{aligned} q'_1 &= 1 - O(\delta_c), \\ q'_2 &= 1 - \varepsilon' - \mathrm{poly}(\varepsilon), \\ q'_3 &= \frac{1}{3} + w - \mathrm{poly}(\varepsilon) - O(\varepsilon'), \\ q'_4 &= 1, \end{aligned}$$

where q'_1, q'_2, q'_3 and q'_4 are their success probabilities in the four types of rounds, and $1-\delta_c$ is the completeness of the RIGID test; from Corollary 3 we have $\delta_c = 2^{-\Omega(n+t)}$. Moreover PV' applies the honest strategy in all rounds, while PP' applies the honest strategy in the Rigidity-Clifford and Rigidity-Tomography rounds. Applying Lemma 35, it follows that

$$w \leq O(\varepsilon') + \mathrm{poly}(\varepsilon) + p_1 \cdot O(\delta_c).$$

Therefore the prover's overall success probability is at most

$$\begin{aligned} &\min(p_1, p_4)(1-\varepsilon) + \max(p_1, p_4) + p_2(1-\varepsilon') + p_3\left(\frac{1}{3} + w\right) \\ \leq &p_{\mathrm{compl}} - \left(\frac{p_3}{3} + \varepsilon' p_2 + \varepsilon \min(p_1, p_4)\right) + p_3\left(O(\varepsilon') + \mathrm{poly}(\varepsilon)\right) + (p_1 + p_3 p_1) \cdot O(\delta_c), \end{aligned}$$

where recall from Lemma 31 that $p_{\mathrm{compl}} = p_1(1-\delta_c) + p_2 + p_4 + \frac{2}{3}p_3$. Fixing p_2 to be a large enough multiple of p_1 and of p_3 we can ensure that the net contribution of the terms involving ε' and δ_c on the right-hand side is always non-positive. Choosing $p_1 = p_4$ and p_3 so that the ratio p_3/p_1 is small enough we can ensure that the right-hand side is less than $p_{\mathrm{compl}} - \Delta$, for some universal constant $\Delta > 0$ and all $\varepsilon, \varepsilon' \geq 0$. □

The Dog-Walker Protocol can be easily extended to a classical-verifier two-prover protocol for all languages in QMA. Along the same lines of the proof that QMIP = MIP* from [82], one of the provers plays the role of PP, running the QMA verification circuit, while the second prover creates and teleports the corresponding QMA witness. In our case, it is not hard to see that the second prover can be re-used as PV in the Dog-Walker Protocol, creating the necessary gadgets for the computation and allowing the Verifier to check the operations performed by the first prover. We refer the reader to the Appendix of [27] for the full details.

4.5.4 Running our protocols in sequence

In order to make a fair comparison between previous delegated computation protocols and ours (see Figure 4.1) we analyzed their resource requirements under the condition that they produce the

correct outcome of the computation with 99% probability. For most protocols, this is achieved by sequentially repeating the original version, in order to amplify the completeness-soundness gap.

In this section, we describe a sequential procedure that, starting from our protocols in Sections 4.5.2 and 4.5.3, ensures that either the verifier aborts, or she obtains the correct outcome of the computation with probability 99%. Moreover, for honest provers, the probability that the procedure aborts is exponentially small in the number of sequential repetitions. Our sequential procedure has a number of rounds which depends on the desired soundness. As long as one only requires amplification of an arbitrarily small, but constant, soundness, to a fixed constant, the number of sequential repetitions remains constant.

To emphasize the importance of having such a sequential procedure, we note that, firstly, the current completeness-soundness gap between acceptance probability on *yes* and *no* instances, for both the leash and the Dog-Walker protocol, is a very small constant. Secondly, if a classical client wishes to employ our protocols to delegate a computation, we need to specify what the client interprets, at the end of the protocol, as the outcome of the delegated computation. The natural approach is to have the verifier interpret a*ccept* as a *yes* outcome and r*eject* as a *no* outcome. However, this is not enough, as our security model based on the constant gap between acceptance probability for *yes* and *no* instances means that, while the provers have a low probability of making the verifier accept a *no* instance as a *yes*, they can always make the verifier accept a *yes* instance as a *no*, simply by behaving so that they are rejected.

The first point is addressed by running copies of the original protocol in sequence to amplify the completeness-soundness gap. The second point is addressed by having the verifier run the protocol twice: once for the circuit Q, and once for the circuit Q' defined by appending an X gate to the output wire of Q. If $f : X \to \{0,1\}$ for some $X \subseteq \{0,1\}^n$ is defined by $f(x) = 1$ if $\|\Pi_0 Q\,|x\rangle\|^2 \geq 2/3$, and $f(x) = 0$ if $\|\Pi_0 Q\,|x\rangle\|^2 \leq 1/3$, i.e. Q decides f with bounded error $1/3$, then it is easy to see that Q' decides $1 - f$ with bounded error $1/3$. Thus, the verifier will accept x as a *yes* instance of f if the protocol outputs a*ccept* when running Q on x and outputs r*eject* when running Q' on x. The verifier accepts x as a *no* instance of f if the protocol outputs r*eject* when running Q on x and outputs a*ccept* when running Q' on x. The verifier aborts if she sees a*ccept*-a*ccept* or r*eject*-r*eject*.

4.5.4.1 Sequential version of our protocols

Let P denote either the Verifier-on-a-leash or the Dog-Walker protocol from Sections 4.5.2 and 4.5.3 respectively, and let c and Δ denote the completeness and completeness-soundness gap. Let κ be a security parameter.

Protocol Seq(P, c, Δ, κ): Let (Q, x) be the verifier's input.

1. The verifier runs κ copies of protocol P in sequence on input (Q, x) with PP and PV. Then she runs κ copies in sequence on input (Q', x).
2. Let $\mathbf{o}, \tilde{\mathbf{o}} \in \{0,1\}^\kappa$ be such that $o_i = 1$ iff the i-th copy on input (Q, x) accepts, and $\tilde{o}_i = 1$ iff the i-th copy on input (Q', x) accepts. Let $wt(\mathbf{o})$ and $wt(\tilde{\mathbf{o}})$ be their Hamming weights. Then, the verifier accepts 1 as the outcome of the delegated computation if $wt(\mathbf{o}) \geq (c - \frac{\Delta}{2}) \cdot \kappa$ and $wt(\tilde{\mathbf{o}}) < (c - \frac{\Delta}{2}) \cdot \kappa$, and she accepts 0 as the outcome of the computation if $wt(\mathbf{o}) < (c - \frac{\Delta}{2}) \cdot \kappa$ and $wt(\tilde{\mathbf{o}}) \geq (c - \frac{\Delta}{2}) \cdot \kappa$. Otherwise the verifier aborts.

Figure 4.26: Sequential version of our protocols

We state and prove completeness and soundness for the sequential protocol.

Theorem 14. *Let c and Δ be respectively the completeness and completeness-soundness gap of protocol P. On input (Q, x):*

- *If the provers are honest,*

$$\Pr\left(Seq(P, c, \Delta, \kappa) \text{ outputs } f(x)\right) \geq 1 - 2\exp\left(-\frac{\Delta^2 \kappa}{2}\right).$$

- *For any cheating provers,*

$$\Pr\left(Seq(P, c, \Delta, \kappa) \text{ outputs } 1 - f(x)\right) \leq \exp\left(-\frac{\Delta^2 \kappa}{8}\right).$$

Proof. We first show completeness. Let $s = c - \Delta$ be the soundness of protocol P. Suppose $f(x) = 1$ (the case $f(x) = 0$ is analogous). If the provers are honest, then the probability that the verifier outputs 1 is:

$$\begin{aligned}
\Pr(\text{Verifier outputs } 1) &= \Pr\left(wt(\mathbf{o}) \geq \left(c - \frac{\Delta}{2}\right) \cdot \kappa \ \wedge \ wt(\tilde{\mathbf{o}}) < \left(c - \frac{\Delta}{2}\right) \cdot \kappa\right) \\
&\geq 1 - \Pr\left(wt(\mathbf{o}) < \left(c - \frac{\Delta}{2}\right) \cdot \kappa\right) - \Pr\left(wt(\tilde{\mathbf{o}}) \geq \left(c - \frac{\Delta}{2}\right) \cdot \kappa\right) \\
&\geq 1 - 2\exp\left(-\frac{\Delta^2 \kappa}{2}\right)
\end{aligned}$$

by Hoeffding's inequality.

Next we show soundness. Again suppose $f(x) = 1$ (the case $f(x) = 0$ is analogous). Let W_j be an indicator random variable for the event $\tilde{o}_j = 1$, and let $F_j = W_j - s$. One might be tempted to

immediately assert that $\mathbb{E}(F_j|F_{j-1},..,F_1) \leq 0$. However, because of the sequentiality of the runs of protocol P, this is not in general true, and an analysis that treats protocol P as a black-box does not suffice when P is the verifier-on-a-leash protocol (because such a protocol is blind). We argue more precisely that $\mathbb{E}(F_j|F_{j-1},..,F_1) \leq 0$:

- When P is the dog-walker protocol from Section 4.5.3 (which is not blind): suppose for a contradiction that there were provers PV and PP, and a j such that $\mathbb{E}(F_j|F_{j-1},..,F_1) \leq 0$. Then one can construct provers PV$'$ and PP$'$ which break the soundness of protocol P. Namely PV$'$ and PP$'$ simulate $j-1$ runs of protocol P. They then respectively invoke PV and PP and forward to them the transcripts previously generated. PV$'$ and PP$'$ then participate in the challenge protocol P by forwarding all of the incoming messages to the invocations of PV and PP respectively. By the initial hypothesis, such PV$'$ and PP$'$ would break the soundness of P.

- When P is the verifier-on-a-leash protocol from Section 4.5.2: the key observation is that protocol P remains sound even when x is revealed to the provers. Then, notice that if it is possible for provers to force $\mathbb{E}(F_j|F_{j-1},..,F_1) \leq 0$ when x is not revealed, it is clearly also possible to do so when x is revealed. However, the latter is not possible, by an analogous reduction to the one for the dog-walker protocol.

Define $X_l = \sum_{j=1}^{l} F_j$, for $l = 1,..,\kappa$. The sequence of X_l's defines a super-martingale with $|X_l - X_{l-1}| = |F_l| \leq 1 \; \forall j$. Hence, by Azuma's inequality, for any $\kappa \geq 1$, $\Pr(X_\kappa \geq t) \leq \exp\left(-\frac{t^2}{2\kappa}\right)$. This implies that

$$\Pr\left(\sum_{j=1}^{\kappa} W_j - \kappa \cdot s \geq t\right) = \Pr\left(\sum_{j=1}^{\kappa} F_j \geq t\right) = \Pr\left(X_\kappa \geq t\right) \leq \exp\left(-\frac{t^2}{2\kappa}\right).$$

Then, for any provers PP and PV,

$$\begin{aligned}
\Pr(\text{Verifier outputs } 0) &\leq \Pr\left(wt(\tilde{\mathbf{o}}) \geq (c - \frac{\Delta}{2}) \cdot \kappa\right) \\
&= \Pr\left(\sum_{j=1}^{\kappa} W_j \geq (c - \frac{\Delta}{2}) \cdot \kappa\right) \\
&= \Pr\left(\sum_{j=1}^{\kappa} W_j - \kappa \cdot s \geq \kappa \cdot \frac{\Delta}{2}\right) \\
&\leq \exp\left(-\frac{\Delta^2 \kappa}{8}\right).
\end{aligned}$$

□

Finally, one can check that when P is the verifier-on-a-leash protocol, then $\mathrm{Seq}(P, c, \Delta, \kappa)$ remains blind. This follows from a similar argument as in the proof of Lemma 30.

Chapter 5

SELF-TESTING AS A MORE GENERAL PHENOMENON

In the previous chapters, we have familiarized ourselves with some of the basic results in the theory of self-testing, and with one important application, namely the delegation of quantum computations. In this chapter we address the following natural question: is self-testing a phenomenon that is limited to a few isolated examples, like EPR pairs, copies of EPR pairs, partially entangled pairs of qubits, or are these instances of a more general phenomenon?

A few other examples of self-testable quantum states are known: the maximally entangled pair of qutrits [83] (via numerical evidence), the partially entangled pair of qutrits that violates maximally the CGLMP_3 inequality [28, 2, 103], and a small class of higher dimensional partially entangled pairs of qudits, through our result on parallel self-testing of tilted EPR pairs from Appendix A. For the multi-partite case, it is known that the three-qubit W state [101, 75] and graph states [59, 75] can be self-tested. Hence, it is clear that self-testing is not an exclusive characteristic of maximally entangled states nor qubit states. However, little is known about self-testing of higher-dimensional entangled states (i.e. pairs of entangled qudits for $d > 2$).

In this chapter, we consider the outstanding open question of whether all bipartite pure entangled quantum states (of finite local dimension) can be self-tested. Building on the framework of Yang and Navascués [102], we answer this question affirmatively with an explicit construction of a family of self-testing correlations, with question sets of size 3 and 4 for Alice and Bob respectively, and answer sets of size d for both (where d is the local dimension). This is one of the main results of this thesis. We argue, additionally, that our correlations self-test not only the state, but also certain ideal measurements. We then extend this result by explicitly describing the first example of a family of Bell inequalities, parametrized by an integer $d \geq 2$, which generalizes the CHSH inequality and self-tests the maximally entangled state of any local dimension d (we refer the reader to Remark 1 for the difference between a self-test via a correlation and a self-test via a Bell inequality or non-local game). In the last part of the chapter, we move to the multipartite setting. The primary difficulty in the case of multipartite states is that they are not guaranteed to have a Schmidt decomposition. The first consequence of this is that there exist multipartite states which are *not* local-unitary-equivalent to their complex conjugates in some basis (something that can never happen in the bipartite case). Since taking the complex conjugate of a quantum strategy is an operation that does not affect the correlation induced by the strategy, we infer that such multipartite states *cannot* be self-tested. Nonetheless, we describe a simple approach to self-test multipartite

states, based on projecting degrees of freedom for all parties but two, and considering the correlation restricted to two parties, inspired by [101]. We show that for any multipartite partially entangled GHZ state, there exists a correlation on question sets of size 2 which self-tests it. We use this result as a building block, combined with techniques from Section 5.1, to show that all multipartite entangled Schmidt-decomposable qudit states, of any local dimension d, can be self-tested.

Organization In Section 5.1, we show the main result of this chapter, that all pure bipartite entangled states can be self-tested. In Section 5.2, we extend this result by formulating it in terms of a Bell inequality, for the maximally entangled case. In Section 5.3, we study the multipartite case.

5.1 All pure bipartite entangled states can be self-tested

5.1.1 The main result

For a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, let its *local dimension* be $\max\{\dim(\mathcal{H}_A), \dim(\mathcal{H}_B)\}$. Our main result is the following.

Theorem 15. *For every pure bipartite entangled state $|\Psi\rangle$ of local dimension $d \geq 2$, there exists a correlations $p^* \in \mathcal{C}_q^{3,4,d,d}$ that self-tests $|\Psi\rangle$. Moreover, p^* also self-tests the ideal measurements described in Subsection 5.1.2.3.*

A $O(poly(d,\epsilon))$-robust version of this result also holds. We refer the reader to the appendix of [25] for the details, which are not included in this thesis.

We will describe the family of correlations that makes Theorem 15 true. We will first give a high-level description. We will follow this by a formal description.

5.1.2 The self-testing correlation

5.1.2.1 The high-level idea

For clarity, in this paragraph we assume d to be even, but the proof will apply to odd d as well.

Since any pure bipartite entangled state possesses a Schmidt decomposition (i.e. is related by a local unitary to a state in Schmidt form), the question of self-testing all pure bipartite entangled states reduces to the question of self-testing an arbitrary bipartite state of the form:

$$|\psi_{\text{target}}\rangle := \sum_{i=0}^{d-1} c_i \, |ii\rangle \ ,$$

where $0 < c_i < 1$ for all i and $\sum_{i=0}^{d-1} c_i^2 = 1$.

The approach, inspired by [102], is to use d-outcome measurements on Alice and Bob's side such that, for some measurement settings, the correlation tables $T_{x,y}$ are block-diagonal with 2×2 blocks. More precisely, for questions $x, y \in \{0,1\}$, the 2×2 blocks will correspond to outcomes a, b respectively in $\{0,1\}$, in $\{2,3\}$,..., in $\{d-2, d-1\}$; the idea is that the m-th 2×2 block "self-tests" the portion $c_{2m} \, |2m \ 2m\rangle + c_{2m+1} \, |2m+1 \ \ 2m+1\rangle$ of the target state. Intuitively, if we were to project the target state onto the subspace spanned by the $2m, 2m+1$ computational basis vectors, we would know how to test this state: we can do so by using the tilted CHSH inequality for the appropriately chosen angle.

Similarly, for questions $x \in \{0,2\}, y \in \{2,3\}$, we let the 2×2 blocks correspond to outcomes a, b respectively in $\{1,2\}$, in $\{3,4\}$,..., in $\{d-1, 0\}$ (i.e. the blocks are shifted forward by

one), again the idea being that the mth block "self-tests" the portion $c_{2m+1}\,|2m+1\ 2m+1\rangle + c_{2m+2}\,|2m+2\ \ 2m+2\rangle$ of the target state.

The 2×2 blocks in our block-diagonal correlation tables, for both subsets of questions, will naturally correspond to ideal tilted CHSH correlations for appropriately chosen angles.

See Fig. 5.1 for an illustration of the concept.

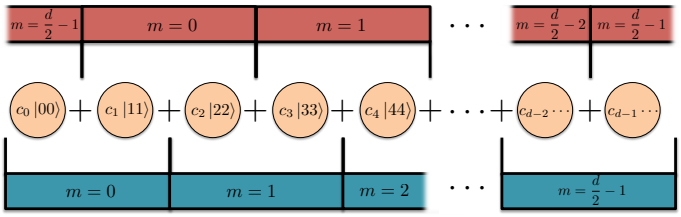


Figure 5.1: In blue, the block-diagonal structure of the correlation tables for questions $x, y \in \{0,1\}$ "certifies" the "even-odd" pairs, while, in red, the block-diagonal structure of the correlation tables for questions $x \in \{0,2\}, y \in \{2,3\}$ certifies the "odd-even" pairs.

It will become clearer, once we describe the self-testing correlation, why the interweaving pattern of the blocks is required.

5.1.2.2 A formal description of the correlation

In order to self-test the target state $|\psi_{\text{target}}\rangle = \sum_{i=0}^{d-1} c_i\,|ii\rangle$, where $0 < c_i < 1$, we will not need to specify the entire self-testing correlation, but it will be enough to specify the correlation tables corresponding to measurement settings $x, y \in \{0,1\}$, and those for settings $x \in \{0,2\}, y \in \{2,3\}$ (recall the definition of a correlation table from Section 2.2). We will show that any correlation satisfying these constraints self-tests $|\psi_{\text{target}}\rangle$. In Subsection 5.1.2.3, we will explicitly provide ideal measurements that satisfy such constraints when acting on $|\psi_{\text{target}}\rangle$. We will refer to the correlation specified by these measurements as the *self-testing correlation* or the *ideal correlation*. The reader may find the description of the ideal measurements achieving these constraints, from Subsection 5.1.2.3, helpful in visualizing the ideal correlation.

Building on an idea of Yang and Navascués [102], the constraints that we impose on the correlation are:

(i) For $x, y \in \{0,1\}$, the correlation tables are block diagonal with 2×2 blocks. The tables for measurement settings $x, y \in \{0,1\}$ are given in Tables 5.1 and 5.2 for even and odd d respectively. The 2×2 blocks $C_{x,y,m}$ are given by $(c_{2m}^2 + c_{2m+1}^2) \cdot C^{\text{ideal}}_{x,y,\theta_m}$

where the $C^{\text{ideal}}_{x,y,\theta_m}$ are the 2×2 correlation tables which correspond to the maximal violation of the tilted-CHSH inequality which self-tests the state $\cos(\theta_m)|00\rangle + \sin(\theta_m)|11\rangle$, where $\theta_m := \arctan\left(\frac{c_{2m+1}}{c_{2m}}\right) \in (0, \frac{\pi}{2})$. They are given precisely in Tables 5.3-5.5, with $\mu_m := \arctan(\sin(2\theta_m))$.

$a\backslash b$	0	1	2	3	$\cdots$	$d-2$	$d-1$
0	$C_{x,y,m=0}$		0	0	$\cdots$	0	0
1			0	0	$\cdots$	0	0
2	0	0	$C_{x,y,m=1}$		$\cdots$	0	0
3	0	0			$\cdots$	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$d-2$	0	0	0	0	$\cdots$	$C_{x,y,m=\frac{d}{2}-1}$	
$d-1$	0	0	0	0	$\cdots$		

Table 5.1: $T_{x,y}$ for $x, y \in \{0,1\}$ for even values of $d \geq 2$

$a\backslash b$	0	1	2	3	$\cdots$	$d-3$	$d-2$	$d-1$
0	$C_{x,y,m=0}$		0	0	$\cdots$	0	0	0
1			0	0	$\cdots$	0	0	0
2	0	0	$C_{x,y,m=1}$		$\cdots$	0	0	0
3	0	0			$\cdots$	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	0
$d-3$	0	0	0	0	$\cdots$	$C_{x,y,m=\frac{d-3}{2}}$		0
$d-2$	0	0	0	0	$\cdots$			0
$d-1$	0	0	0	0	$\cdots$	0	0	c^2_{d-1}

Table 5.2: $T_{x,y}$ for $x, y \in \{0,1\}$ for odd values of $d \geq 3$

$a\backslash b$	2m	2m+1
2m	$c^2_{2m}\cos^2\left(\frac{\mu_m}{2}\right)$	$c^2_{2m}\sin^2\left(\frac{\mu_m}{2}\right)$
2m+1	$c^2_{2m+1}\sin^2\left(\frac{\mu_m}{2}\right)$	$c^2_{2m+1}\cos^2\left(\frac{\mu_m}{2}\right)$

Table 5.3: 2×2 block correlation table $C_{x=0,y=0,m}$ and $C_{x=0,y=1,m}$

$a\backslash b$	2m	2m+1
2m	$\frac{1}{2}(c_{2m}\cos(\frac{\mu_m}{2})+c_{2m+1}\sin(\frac{\mu_m}{2}))^2$	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m}{2})-c_{2m}\sin(\frac{\mu_m}{2}))^2$
2m+1	$\frac{1}{2}(c_{2m}\cos(\frac{\mu_m}{2})-c_{2m+1}\sin(\frac{\mu_m}{2}))^2$	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m}{2})+c_{2m}\sin(\frac{\mu_m}{2}))^2$

Table 5.4: 2×2 block correlation table $C_{x=1,y=0,m}$

$a\backslash b$	2m	2m+1
2m	$\frac{1}{2}(c_{2m}\cos(\frac{\mu_m}{2})-c_{2m+1}\sin(\frac{\mu_m}{2}))^2$	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m}{2})+c_{2m}\sin(\frac{\mu_m}{2}))^2$
2m+1	$\frac{1}{2}(c_{2m}\cos(\frac{\mu_m}{2})+c_{2m+1}\sin(\frac{\mu_m}{2}))^2$	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu_m}{2})-c_{2m}\sin(\frac{\mu_m}{2}))^2$

Table 5.5: 2×2 block correlation table $C_{x=1,y=1,m}$

(ii) Similarly, for measurement settings $x\in\{0,2\}$ and $y\in\{2,3\}$ the correlation tables $T_{x,y}$ are also block-diagonal, but "shifted down" appropriately by one measurement outcome. The 2×2 blocks are $D_{x,y,m}$ (corresponding to outcomes $2m+1$ and $2m+2$) for $x\in\{0,2\}$ and $y\in\{2,3\}$, defined as $D_{x,y,m}:=(c_{2m+1}^2+c_{2m+2}^2)\cdot C^{ideal}_{f(x),g(y);\theta'_m}$, where $\theta'_m:=\arctan\left(\frac{c_{2m+2}}{c_{2m+1}}\right)\in(0,\frac{\pi}{2})$, and $f(0)=0, f(2)=1, g(2)=0, g(3)=1$. The correlations, $T_{x,y}$, for $x\in\{0,2\}$ and $y\in\{2,3\}$ are given precisely in Tables 5.6 to 5.10 where $\mu'_m:=\arctan(\sin(2\theta'_m))$.

<table>
<tr><th>$a\backslash b$</th><th>1</th><th>2</th><th>3</th><th>4</th><th>$\cdots$</th><th>$d-1$</th><th>0</th></tr>
<tr><td>1</td><td colspan="2" rowspan="2">$D_{x,y,m=0}$</td><td>0</td><td>0</td><td>$\cdots$</td><td>0</td><td>0</td></tr>
<tr><td>2</td><td>0</td><td>0</td><td>$\cdots$</td><td>0</td><td>0</td></tr>
<tr><td>3</td><td>0</td><td>0</td><td colspan="2" rowspan="2">$D_{x,y,m=1}$</td><td>$\cdots$</td><td>0</td><td>0</td></tr>
<tr><td>4</td><td>0</td><td>0</td><td>$\cdots$</td><td>0</td><td>0</td></tr>
<tr><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td><td>$\ddots$</td><td>$\vdots$</td><td>$\vdots$</td></tr>
<tr><td>$d-1$</td><td>0</td><td>0</td><td>0</td><td>0</td><td>$\cdots$</td><td colspan="2" rowspan="2">$D_{x,y,m=\frac{d}{2}-1}$</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>$\cdots$</td></tr>
</table>

Table 5.6: $T_{x,y}$ for $x\in\{0,2\}$ and $y\in\{2,3\}$, for even values of $d\geq 2$

$a\backslash b$	1	2	3	4	$\cdots$	$d-2$	$d-1$	0
1	$D_{x,y,m=0}$		0	0	$\cdots$	0	0	0
2			0	0	$\cdots$	0	0	0
3	0	0	$D_{x,y,m=1}$		$\cdots$	0	0	0
4	0	0			$\cdots$	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	0
$d-2$	0	0	0	0	$\cdots$	$D_{x,y,m=\frac{d-3}{2}}$		0
$d-1$	0	0	0	0	$\cdots$			0
0	0	0	0	0	$\cdots$	0	0	c_0^2

Table 5.7: $T_{x,y}$ for $x \in \{0,2\}$ and $y \in \{2,3\}$, for odd values of $d \geq 3$

$a\backslash b$	2m+1	2m+2
2m+1	$c_{2m+1}^2 \cos^2(\frac{\mu'_m}{2})$	$c_{2m+1}^2 \sin^2(\frac{\mu'_m}{2})$
2m+2	$c_{2m+2}^2 \sin^2(\frac{\mu'_m}{2})$	$c_{2m+2}^2 \cos^2(\frac{\mu'_m}{2})$

Table 5.8: 2×2 block correlation table $D_{x=0,y=2,m}$ and $D_{x=0,y=3,m}$

$a\backslash b$	2m+1	2m+2
2m+1	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu'_m}{2}) + c_{2m+2}\sin(\frac{\mu'_m}{2}))^2$	$\frac{1}{2}(c_{2m+2}\cos(\frac{\mu'_m}{2}) - c_{2m+1}\sin(\frac{\mu'_m}{2}))^2$
2m+2	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu'_m}{2}) - c_{2m+2}\sin(\frac{\mu'_m}{2}))^2$	$\frac{1}{2}(c_{2m+2}\cos(\frac{\mu'_m}{2}) + c_{2m+1}\sin(\frac{\mu'_m}{2}))^2$

Table 5.9: 2×2 block correlation table $D_{x=2,y=2,m}$

$a\backslash b$	2m+1	2m+2
2m+1	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu'_m}{2}) - c_{2m+2}\sin(\frac{\mu'_m}{2}))^2$	$\frac{1}{2}(c_{2m+2}\cos(\frac{\mu'_m}{2}) + c_{2m+1}\sin(\frac{\mu'_m}{2}))^2$
2m+2	$\frac{1}{2}(c_{2m+1}\cos(\frac{\mu'_m}{2}) + c_{2m+2}\sin(\frac{\mu'_m}{2}))^2$	$\frac{1}{2}(c_{2m+2}\cos(\frac{\mu'_m}{2}) - c_{2m+1}\sin(\frac{\mu'_m}{2}))^2$

Table 5.10: 2×2 block correlation table $D_{x=2,y=3,m}$

5.1.2.3 The ideal measurements

We now explicitly provide the ideal measurements on $|\psi_{\text{target}}\rangle = \sum_{i=0}^{d-1} c_i |ii\rangle$ that satisfy the constraints described above, and we refer to the correlation produced by the ideal measurements as the *ideal correlation*.

Let σ_Z and σ_X be the usual Pauli matrices. For a single-qubit observable A, we denote by $[A]_m$ the observable defined with respect to the basis $\{|2m \mod d\rangle, |(2m+1) \mod d\rangle\}$. For example, $[\sigma_Z]_m = |2m\rangle\langle 2m| - |2m+1\rangle\langle 2m+1|$. Similarly, we denote by $[A]'_m$ the observable defined with respect to the basis $\{|(2m+1) \mod d\rangle, |(2m+2) \mod d\rangle\}$. We use the notation $\bigoplus A_i$ to denote the direct sum of observables A_i.

For $x = 0$: Alice measures in the computational basis (i.e. in the basis $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$). For $x = 1$ and $x = 2$: for d even, she measures in the eigenbases of observables $\bigoplus_{m=0}^{\frac{d}{2}-1}[\sigma_X]_m$ and $\bigoplus_{m=0}^{\frac{d}{2}-1}[\sigma_X]'_m$ respectively, with the natural assignments of d measurement outcomes; for d odd, she measures in the eigenbases of observables $\bigoplus_{m=0}^{\frac{d-1}{2}-1}[\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ and $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1}[\sigma_X]'_m$ respectively.

In a similar way, for $y = 0$ and $y = 1$: for d even, Bob measures in the eigenbases of $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu_m)\sigma_Z + \sin(\mu_m)\sigma_X]_m$ and $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu_m)\sigma_Z - \sin(\mu_m)\sigma_X]_m$ respectively, with the natural assignments of d measurement outcomes, where here $\mu_m = \arctan(\sin(2\theta_m))$ and $\theta_m = \arctan\left(\frac{c_{2m+1}}{c_{2m}}\right)$; for d odd, he measures in the eigenbases of $\bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu_m)\sigma_Z + \sin(\mu_m)\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ and $\bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu_m)\sigma_Z - \sin(\mu_m)\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ respectively.

For $y = 2$ and $y = 3$: for d even, Bob measures in the eigenbases of $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu'_m)\sigma_Z + \sin(\mu'_m)\sigma_X]'_m$ and $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu'_m)\sigma_Z - \sin(\mu'_m)\sigma_X]'_m$ respectively, where $\mu'_m = \arctan(\sin(2\theta'_m))$ and $\theta'_m = \arctan\left(\frac{c_{2m+2}}{c_{2m+1}}\right)$; for d odd, he measures in the eigenbases of $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu'_m)\sigma_Z + \sin(\mu'_m)\sigma_X]'_m$ and $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu'_m)\sigma_Z - \sin(\mu'_m)\sigma_X]'_m$ respectively.

Before proceeding to the proof of Theorem 15, we state a technical lemma that we will employ in the proof.

5.1.3 Sufficient conditions for self-testing an entangled pair of qudits

Before proceeding to the proof of Theorem 15, we state state a (slightly more general) version of a Lemma from Yang and Navascués [102], which gives a sufficient criterion for self-testing a general pure bipartite entangled state.

Lemma 37. *Let $|\psi_{target}\rangle = \sum_{i=0}^{d-1} c_i |ii\rangle$, where $0 < c_i < 1$ for all i and $\sum_{i=0}^{d-1} c_i^2 = 1$. Suppose there exist unitary operators $X_A^{(k)}, X_B^{(k)}$ and projections $\{P_A^{(k)}\}_{k=0,..,d-1}$ and $\{P_B^{(k)}\}_{k=0,..,d-1}$ of which $\{P_A^{(k)}\}_{k=0,..,d-1}$ is a complete orthogonal set, while $\{P_B^{(k)}\}_{k=0,..,d-1}$ need not be, and they*

satisfy the following conditions:

$$P_A^{(k)} |\psi\rangle = P_B^{(k)} |\psi\rangle \quad \forall k, \tag{5.1}$$

$$X_A^{(k)} X_B^{(k)} P_B^{(k)} |\psi\rangle = \frac{c_k}{c_0} P_A^{(0)} |\psi\rangle \quad \forall k \tag{5.2}$$

Then there exists a local isometry Φ *such that* $\Phi(|\psi\rangle) = |extra\rangle \otimes |\psi_{target}\rangle$*, for some auxiliary state* $|extra\rangle$*.*

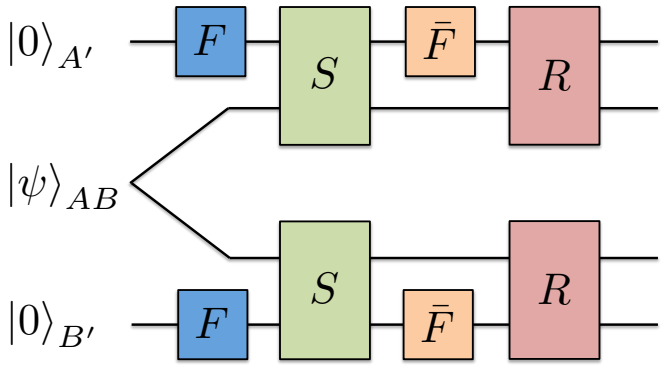


Figure 5.2: Diagram of the isometry $\Phi(|\psi\rangle)$

The complete proof of this is given in Appendix B.1. The Lemma also holds when $|\psi\rangle$ is replaced by a general mixed state ρ, and equalities between vectors are naturally replaced by equalities between density matrices, as is clear from the proof in Appendix B.1. Here we just describe how the local isometry Φ is constructed (Fig. 5.2). The local isometry adds two ancilla qudits in the zero state, and is a generalization of the *swap isometry* that we encountered in Section 3.3 for the qubit case. More precisely,

$$\Phi(|\psi\rangle) = (R_{AA'} \otimes R_{BB'})(\bar{F}_{A'} \otimes \bar{F}_{B'})(S_{AA'} \otimes S_{BB'})(F_{A'} \otimes F_{B'}) |\psi\rangle_{AB} |0\rangle_{A'} |0\rangle_{B'} ,$$

where F is the quantum Fourier transform, $\bar{F}$ is the inverse quantum Fourier transform, $R_{AA'/BB'}$ is defined as $R_{AA'/BB'} |\psi\rangle_{AB} |k\rangle_{A'/B'} = X_{A/B}^{(k)} |\psi\rangle_{AB} |k\rangle_{A'/B'}$ and $S_{AA'/BB'}$ is defined as $S_{AA'/BB'} |\psi\rangle_{AB} |k\rangle_{A'/B'} = Z_{A/B}^{k} |\psi\rangle_{AB} |k\rangle_{A'/B'}$. Yang and Navascués [102] did not provide, or prove the existence of, correlations from which one can construct operators satisfying the conditions of Lemma 37, and this is our main contribution.

5.1.4 Proof of self-testing

This section is dedicated entirely to proving Theorem 15. Most of the work in the proof is aimed at constructing operators satisfying the sufficient conditions from Lemma 37. This, explicitly, means

constructing appropriate projections $P_A^{(k)}, P_B^{(k)}$ and unitaries $X_A^{(k)}, X_B^{(k)}$. In Subsection 5.1.4.1, we construct the projections, and, moreover, certain unitary "flip" operators $X_{A,m}, X'_{A,m}$. In Subsection 5.1.4.2, we show how to obtain unitaries $X_A^{(k)}, X_B^{(k)}$ as appropriate alternating products of the flip operators. Finally, we argue that the same local isometry given by Lemma 37 works also to self-test the ideal measurements from Subsection 5.1.2.3.

5.1.4.1 Constructing the projections and the "flip" operators

Recall that we denote by $\Pi_i^{A_x}$ the projection corresponding to Alice obtaining outcome i on measurement setting x, and similarly for the $\Pi_i^{B_y}$ on Bob's side. We will first derive consequences that follow from the constraints in item (i) of Subsection 5.1.2.2, that we imposed on our correlations. The constraints in item (ii) of Subsection 5.1.2.2 have similar implications.

We define the operators $\hat{A}_{x,m} = \Pi_{2m}^{A_x} - \Pi_{2m+1}^{A_x}$ and $\hat{B}_{y,m} = \Pi_{2m}^{B_y} - \Pi_{2m+1}^{B_y}$ for $x, y \in \{0,1\}$. Clearly, $(\hat{A}_{x,m})^2 = \Pi_{2m}^{A_x} + \Pi_{2m+1}^{A_x} := \mathbb{1}_m^{A_x}$ and $(\hat{B}_{y,m})^2 = \Pi_{2m}^{B_y} + \Pi_{2m+1}^{B_y} := \mathbb{1}_m^{B_y}$.
Now, $\|\Pi_{2m}^{A_0}|\psi\rangle\| = \sqrt{\left\langle \psi \middle| \Pi_{2m}^{A_0} \middle| \psi \right\rangle} = \sqrt{\left\langle \psi \middle| \Pi_{2m}^{A_0} \cdot \sum_{i=0}^{d-1} \Pi_i^{B_0} \middle| \psi \right\rangle} = \sqrt{c_{2m}^2 \cos^2\left(\frac{\mu_m}{2}\right) + c_{2m}^2 \sin^2\left(\frac{\mu_m}{2}\right)} = c_{2m}$, and $\|\Pi_{2m+1}^{A_0}|\psi\rangle\| = c_{2m+1}$. With similar other calculations we deduce that

$$\|\mathbb{1}_m^{A_i}|\psi\rangle\| = \|\mathbb{1}_m^{B_j}|\psi\rangle\| = \sqrt{c_{2m}^2 + c_{2m+1}^2} \quad \forall i,j \in \{0,1\}\,. \tag{5.3}$$

Moreover, notice that $\left\langle \psi \middle| \mathbb{1}_m^{A_i}\mathbb{1}_m^{B_j} \middle| \psi \right\rangle = c_{2m}^2 + c_{2m+1}^2 = \|\mathbb{1}_m^{A_i}|\psi\rangle\| \cdot \|\mathbb{1}_m^{B_j}|\psi\rangle\|$. Hence, by Cauchy-Schwarz, it must be the case that

$$\mathbb{1}_m^{A_i}|\psi\rangle = \mathbb{1}_m^{B_j}|\psi\rangle \quad \forall i,j \in \{0,1\}\,. \tag{5.4}$$

By design, the correlations are such that

$$\langle\psi|\, \alpha_m \hat{A}_{0,m} + \hat{A}_{0,m}\hat{B}_{0,m} + \hat{A}_{0,m}\hat{B}_{1,m} + \hat{A}_{1,m}\hat{B}_{0,m} - \hat{A}_{1,m}\hat{B}_{1,m}\,|\psi\rangle = \sqrt{8 + 2\alpha_m^2}\cdot(c_{2m}^2 + c_{2m+1}^2)\,,$$

where $\alpha_m = \frac{2}{\sqrt{1+2\tan^2(2\theta_m)}}$. As such, this is not a maximal violation of the tilted CHSH inequality (since $|\psi\rangle$ has unit norm). However, we can get around this by defining the normalized state $|\psi_m\rangle = \frac{\mathbb{1}_m^{A_0}|\psi\rangle}{\sqrt{c_{2m}^2+c_{2m+1}^2}}$. Since $\hat{A}_{i,m}|\psi\rangle = \hat{A}_{i,m}\mathbb{1}_m^{A_i}|\psi\rangle = \hat{A}_{i,m}\mathbb{1}_m^{A_0}|\psi\rangle$, and $\hat{B}_{i,m}|\psi\rangle = \hat{B}_{i,m}\mathbb{1}_m^{B_i}|\psi\rangle = \hat{B}_{i,m}\mathbb{1}_m^{A_0}|\psi\rangle$, by (5.4), then (5.1.4.1) implies =

$$\langle\psi_m|\, \alpha_m \hat{A}_{0,m} + \hat{A}_{0,m}\hat{B}_{0,m} + \hat{A}_{0,m}\hat{B}_{1,m} + \hat{A}_{1,m}\hat{B}_{0,m} - \hat{A}_{1,m}\hat{B}_{1,m}\,|\psi_m\rangle = \sqrt{8 + 2\alpha_m^2}\,. \tag{5.5}$$

Now, define the "unitarized" versions of the operators in (5.5): $\hat{A}_{i,m} := \mathbb{1} - \mathbb{1}_m^{A_i} + \hat{A}_{i,m}$ and $\hat{B}_{i,m} := \mathbb{1} - \mathbb{1}_m^{B_i} + \hat{B}_{i,m}$. Then clearly equation (5.5) holds also with the unitarized operators, by definition of $|\psi_m\rangle$. Now, let $Z_{A,m} := \hat{A}_{0,m}$, $X_{A,m} := \hat{A}_{1,m}$. Then, on Bob's side, we again need to perform the following unitarization step. Let $\hat{B}_{0,m} + \hat{B}_{1,m} + \mathbb{1}_{\mathrm{Ker}(\hat{B}_{0,m}+\hat{B}_{1,m})} = U^+\Pi^+$ and $\hat{B}_{0,m} - \hat{B}_{1,m} + \mathbb{1}_{\mathrm{Ker}(\hat{B}_{0,m}-\hat{B}_{1,m})} = U^-\Pi^-$ be polar decompositions. Define $Z_{B,m} = U^+$ and $X_{B,m} = U^-$. Then, by Lemma 3, the above maximal violation of the tilted CHSH inequality implies that

$$Z_{A,m}\,|\psi_m\rangle = Z_{B,m}\,|\psi_m\rangle \tag{5.6}$$

$$X_{A,m}(\mathbb{1} - Z_{A,m})\,|\psi_m\rangle = \tan(\theta_m) X_{B,m}(\mathbb{1} + Z_{A,m})\,|\psi_m\rangle\ . \tag{5.7}$$

Define the subspace $\mathcal{B}_m = \mathrm{range}(\mathbb{1}_m^{B_0}) + \mathrm{range}(\mathbb{1}_m^{B_1})$, and the projection $\mathbb{1}_{\mathcal{B}_m}$ onto subspace $\mathcal{B}_m$. Then, notice from the way $Z_{B,m}$ is defined, that it can be written as $Z_{B,m} = \mathbb{1} - \mathbb{1}_{\mathcal{B}_m} + \tilde{Z}_{B,m}$, where $\tilde{Z}_{B,m}$ is some operator living entirely on subspace $\mathcal{B}_m$. This implies that $Z_{B,m}\,|\psi_m\rangle = \tilde{Z}_{B,m}\,|\psi_m\rangle = \tilde{Z}_{B,m}\,|\psi\rangle$, where we have used (5.4) and the fact that

$$\mathbb{1}_m^{B_0}\,|\psi\rangle = \mathbb{1}_m^{B_1}\,|\psi\rangle \implies \mathbb{1}_{\mathcal{B}_m}\,|\psi\rangle = \mathbb{1}_m^{B_i}\,|\psi\rangle\ .$$

Hence, from (5.6) we deduce that $\hat{A}_{0,m}\,|\psi\rangle = \tilde{Z}_{B,m}\,|\psi\rangle$. Define projections $P_A^{(2m)} := (\mathbb{1}_m^{A_0} + \hat{A}_{0,m})/2 = \Pi_{2m}^{A_0}$, $P_A^{(2m+1)} := (\mathbb{1}_m^{A_0} - \hat{A}_{0,m})/2 = \Pi_{2m+1}^{A_0}$, $P_B^{(2m)} := (\mathbb{1}_{\mathcal{B}_m} + \tilde{Z}_{B,m})/2$ and $P_B^{(2m+1)} := (\mathbb{1}_{\mathcal{B}_m} - \tilde{Z}_{B,m})/2$.

Note that $P_B^{(2m)}, P_B^{(2m+1)}$ are indeed projections, since $\tilde{Z}_{B,m}$ has all ± 1 eigenvalues corresponding to subspace $\mathcal{B}_m$, and is zero outside. We also have, for all m and $k = 2m, 2m+1$,

$$\begin{aligned} P_A^{(k)}\,|\psi\rangle = (\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m})/2\,|\psi\rangle &= (\mathbb{1}_m^{B_0} + (-1)^k \hat{A}_{0,m})/2\,|\psi\rangle \\ &= (\mathbb{1}_{\mathcal{B}_m} + (-1)^k \tilde{Z}_{B,m})/2\,|\psi\rangle = P_B^{(k)}\,|\psi\rangle\ . \end{aligned} \tag{5.9}$$

Further, notice that $(\mathbb{1} + (-1)^k Z_{A,m})\,|\psi_m\rangle = (\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m})\,|\psi_m\rangle = (\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m})\,|\psi\rangle = P_A^{(k)}\,|\psi\rangle$. Plugging this into (5.7), gives

$$X_{A,m} P_A^{(2m+1)}\,|\psi\rangle = \tan(\theta_m) X_{B,m} P_A^{(2m)}\,|\psi\rangle = \frac{c_{2m+1}}{c_{2m}} X_{B,m} P_A^{(2m)}\,|\psi\rangle\ .$$

Now, we turn to the constraints on our correlations that we imposed in item (ii) of Subsection 5.1.2.2. These have similar implications to the ones we just derived.

We can similarly define the operators $\hat{A}'_{0,m} = \Pi_{2m+1}^{A_0} - \Pi_{2m+2}^{A_0}$, $\hat{A}'_{1,m} = \Pi_{2m+1}^{A_2} - \Pi_{2m+2}^{A_2}$ $\hat{B}'_{0,m} = \Pi_{2m+1}^{B_2} - \Pi_{2m+2}^{B_2}$, $\hat{B}'_{1,m} = \Pi_{2m+1}^{B_3} - \Pi_{2m+2}^{B_3}$, and $\mathbb{1}_m^{A'_x} = \left(\hat{A}'_{x,m}\right)^2$ and $\mathbb{1}_m^{B'_y} = \left(\hat{B}'_{y,m}\right)^2$. Using

the argument employed earlier and following the same procedure, we can analogously construct unitary operators $Z'_{A,m}$, $X'_{A,m}$, $Z'_{B,m}$ and $X'_{B,m}$ from operators $\hat{A}'_{x,m}$ and $\hat{B}'_{y,m}$.

$$Z'_{A,m}\left|\psi'_m\right\rangle = Z'_{B,m}\left|\psi'_m\right\rangle$$
$$X'_{A,m}(\mathbb{1}_m^{A'_0} - Z'_{A,m})\left|\psi'_m\right\rangle = \tan(\theta'_m)\, X'_{B,m}(\mathbb{1}_m^{A'_0} + Z'_{A,m})\left|\psi'_m\right\rangle \ ,$$

where $|\psi'_m\rangle = \frac{\mathbb{1}_m^{A'_0}|\psi\rangle}{\sqrt{c_{2m+1}^2+c_{2m+2}^2}}$. And from here, with the same steps as above, we deduce that

$$X'_{A,m}P_A^{(2m+2)}\left|\psi\right\rangle = \tan(\theta'_m)\, X'_{B,m}P_A^{(2m+1)}\left|\psi\right\rangle = \frac{c_{2m+2}}{c_{2m+1}}X'_{B,m}P_A^{(2m+1)}\left|\psi\right\rangle \ . \tag{5.10}$$

5.1.4.2 Constructing the unitaries

For notational convenience, we drop the superscript from the unitary operators $X_{A/B,m}$,$X'_{A/B,m}$ in equations (5.7) and (5.10) of the previous subsection. We also rename $X'_{A/B,m}$ as $Y_{A/B,m}$. Then, we recall equations (5.7) and (5.10):

$$X_{A,m}P_A^{2m+1}\left|\psi\right\rangle = \frac{c_{2m+1}}{c_{2m}}X_{B,m}P_A^{2m}\left|\psi\right\rangle \tag{5.11}$$
$$Y_{A,m}P_A^{2m+2}\left|\psi\right\rangle = \frac{c_{2m+2}}{c_{2m+1}}Y_{B,m}P_A^{2m+1}\left|\psi\right\rangle \ . \tag{5.12}$$

Recall that we ultimately wish to produce unitary operators satisfying condition (5.2) from Lemma 37. The operators $X_{A/B,m}$ and $Y_{A/B,m}$ can be can be intuitively thought of as "flip operators", in the sense that $X_{A,m}$ acts on $P_A^{(2m+1)}\left|\psi\right\rangle$ (which is equal to $P_B^{(2m+1)}\left|\psi\right\rangle$ when condition (5.1) is satisfied) and turns it into $X_{B,m}P_A^{(2m)}\left|\psi\right\rangle$, up to an appropriate factor. On the other hand, the flip operator $Y_{A,m}$ will turn $P_A^{(2m)}\left|\psi\right\rangle$ into $Y_{B,m}P_A^{(2m-1)}\left|\psi\right\rangle$, up to a factor. The idea is, then, that the appropriate alternating product of these unitary flip operators will turn $P_A^{(i)}\left|\psi\right\rangle$ into precisely $\frac{c_i}{c_0}(X_B^{(i)})^\dagger P_A^{(0)}\left|\psi\right\rangle$, which is the behaviour required from condition (5.2) of Lemma 37, when we let these alternating products be the $X_A^{(i)}$ and $X_B^{(i)}$ from (5.2).

We have already shown, in (5.9), that the $P_{A/B}^{(k)}$, as defined in the previous subsection, satisfy $P_A^{(k)}\left|\psi\right\rangle = P_B^{(k)}\left|\psi\right\rangle$ for $k = 0, .., d-1$, i.e. condition (5.1) from Lemma 37, with the $P_A^{(k)}$ forming, by definition, a complete set of orthogonal projections.

We are ready to define $X^{(k)}_{A/B}$ as follows:

$$X^{(k)}_A = \begin{cases} \mathbb{1}, & \text{if } k = 0 \\ X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}Y_{A,m-1}X_{A,m} & \text{if } k = 2m+1 \\ X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}Y_{A,m-1}, & \text{if } k = 2m \end{cases}$$

and

$$X^{(k)}_B = \begin{cases} \mathbb{1}, & \text{if } k = 0 \\ X_{B,0}Y_{B,0}X_{B,1}Y_{B,1}\dots X_{B,m-1}Y_{B,m-1}X_{B,m} & \text{if } k = 2m+1 \\ X_{B,0}Y_{B,0}X_{B,1}Y_{B,1}\dots X_{B,m-1}Y_{B,m-1}, & \text{if } k = 2m\,. \end{cases}$$

Note that $X^{(k)}_A$ and $X^{(k)}_B$ are unitary since they are product of unitaries. Finally we check that condition (5.2) holds, namely

$$X^{(k)}_A P^{(k)}_A \left|\psi\right\rangle = \frac{c_k}{c_0}(X^{(k)}_B)^\dagger P^{(0)}_A \left|\psi\right\rangle\,. \tag{5.13}$$

For the case $k = 0$,

$$\begin{aligned} X^{(0)}_A P^{(0)}_A \left|\psi\right\rangle &= \mathbb{1} P^{(0)}_A \left|\psi\right\rangle \\ &= \frac{c_0}{c_0} X^{(0)}_B P^{(0)}_A \left|\psi\right\rangle\,. \end{aligned}$$

For $k = 2m+1$,

$$\begin{aligned} X^{(k)}_A P^{(k)}_A \left|\psi\right\rangle &= X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}Y_{A,m-1}X_{A,m}P^{(2m+1)}_A \left|\psi\right\rangle \\ &\overset{(5.11)}{=} \frac{c_{2m+1}}{c_{2m}} X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}Y_{A,m-1}X_{B,m}P^{(2m)}_A \left|\psi\right\rangle \\ &= \frac{c_{2m+1}}{c_{2m}} X_{B,m}X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}Y_{A,m-1}P^{(2m)}_A \left|\psi\right\rangle \\ &\overset{(5.12)}{=} \frac{c_{2m+1}}{c_{2m}} \cdot \frac{c_{2m}}{c_{2m-1}} X_{B,m}X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}Y_{B,m-1}P^{(2m-1)}_A \left|\psi\right\rangle \\ &= \frac{c_{2m+1}}{c_{2m}} \cdot \frac{c_{2m}}{c_{2m-1}} X_{B,m}Y_{B,m-1}X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}P^{(2m-1)}_A \left|\psi\right\rangle \\ &= \dots \\ &= \frac{c_{2m+1}}{\cancel{c_{2m}}} \cdot \frac{\cancel{c_{2m}}}{\cancel{c_{2m-1}}} \dots \frac{\cancel{c_2}}{\cancel{c_1}} \cdot \frac{\cancel{c_1}}{c_0} X_{B,m}Y_{B,m-1}X_{B,m-1}\dots Y_{B,1}X_{B,1}Y_{B,0}X_{B,0}P^{(0)}_A \left|\psi\right\rangle \\ &= \frac{c_{2m+1}}{c_0}(X^{(k)}_B)^\dagger P^{(0)}_A \left|\psi\right\rangle\,, \end{aligned}$$

which is indeed (5.13), as $2m+1 = k$. The case $k = 2m$ is treated similarly. This completes the construction of the local isometry Φ, by Lemma 37. To conclude the proof of Theorem 15, we just

need to show that this isometry also self-tests the ideal measurements given precisely below. The rest of the proof is included in Appendix B.2.

We emphasize that the whole proof goes through in the same way if we replace $|\psi\rangle$ with a general mixed state. In particular, one simply replaces all equalities between vectors with equalities between density matrices. Moreover, the Euclidean inner product is replaced by $\langle \cdot, \cdot \rangle : \mathcal{L}(\text{supp}\rho, \mathcal{H}_A \otimes \mathcal{H}_B) \times \mathcal{L}(\text{supp}\rho, \mathcal{H}_A \otimes \mathcal{H}_B) \to \mathbb{C}$ such that

$$\langle A, B \rangle := Tr(AB^\dagger \rho),$$

where $\text{supp}\rho = \{|\phi\rangle \in \mathcal{H} : \rho\,|\phi\rangle \neq 0\}$, and $\mathcal{L}(\text{supp}\rho, \mathcal{H}_A \otimes \mathcal{H}_B)$ is the space of linear maps from $\text{supp}\rho$ to $\mathcal{H}_A \otimes \mathcal{H}_B$. Notice that the product defined above doesn't in general satisfy the symmetric property of inner products. Nonetheless, Cauchy-Schwarz still holds on instances that satisfy the symmetry property (in particular when A and B commute). So, as an example, we would replace the expression $\left\langle \psi \middle| \mathbb{1}_m^{A_i} \mathbb{1}_m^{B_j} \middle| \psi \right\rangle$, after equation (5.3), with $\langle \mathbb{1}_m^{A_i}|_{\text{supp}\rho}, \mathbb{1}_m^{B_j}|_{\text{supp}\rho} \rangle = Tr(\mathbb{1}_m^{A_i}|_{\text{supp}\rho} \mathbb{1}_m^{B_j}|_{\text{supp}\rho}\, \rho)$, and deduce, through Cauchy-Schwarz, that $\mathbb{1}_m^{A_i}|_{\text{supp}\rho} = \mathbb{1}_m^{B_j}|_{\text{supp}\rho}$.

Finally, Lemmas 2 and 3, from Bamps and Pironio [7], as well as Lemma 37, hold analogously in corresponding mixed state form.

5.1.5 Discussion

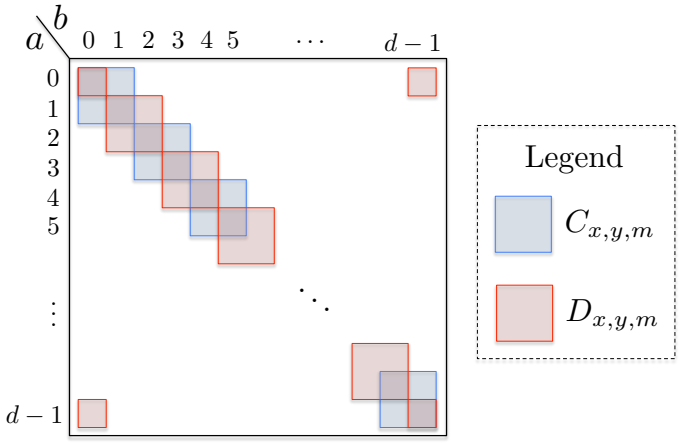


Figure 5.3: Block-diagonal structure of the correlation tables

In our proof, we described explicit self-testing correlations for the 2×2 blocks, in Tables 5.3-5.5 and 5.8-5.10. However, we remark that this is not the only choice of correlations that can be made to self-test all bipartite entangled states. In fact, as a natural consequence of our work, it is the case that any block-diagonal correlations (as in Fig. 5.3) suffice as long as the 2×2 "un-normalized" correlations $C_{x,y,m}$ and $D_{x,y,m}$ imply the existence of reflections Z_A, X_A on Alice's side and Z_B, X_B

on Bob's side such that

$$Z_A |\psi\rangle = Z_B |\psi\rangle \tag{5.14}$$

$$X_A(\mathbb{1} - Z_A) |\psi\rangle = \tan(\theta) X_B(\mathbb{1} + Z_A) |\psi\rangle \tag{5.15}$$

for appropriate angles θ. For instance, in order to self-test bipartite maximally entangled states, we can invoke any correlation in the class given by Wang et al. [99] where $A_0 |\psi\rangle = B_0 |\psi\rangle$ (in the notation of Ref [99], $\alpha_{00} = 0$). These correlations satisfy equations (5.14) and (5.15) for $\tan\theta = 1$: thus, they can be used to self-test the maximally entangled pair of qudits, for any d, as is suggested by Yang and Navascués [102]. For these correlations, notice, moreover, that for $x = 0, y = 0$, the correlation table is diagonal and hence, we can drop Bob's fourth measurement setting because a diagonal correlation can fulfil its role as both $C_{x,y,m}$ and $D_{x,y,m}$. Thus, one can self-test maximally entangled states of arbitrary dimension with question sets of size 3 and answer sets of size d.

5.2 A generalization of the CHSH inequality self-testing maximally entangled states of any local dimension

In the previous section, we saw that for any pure bipartite entangled state, there exists a correlation that self-tests it. In this section, we seek to *upgrade* the self-test via a correlation to a self-test via a non-local game. In practice having a self-test via a non-local game is useful, because one only needs to estimate a *single number*, namely the Bell violation or the value in the game, as opposed to having to estimate the full correlation. Our plan is the following: for each bipartite entangled state $|\Psi\rangle$, we wish to write down a Bell inequality (or equivalently a non-local game), which achieves its maximum violation uniquely at the self-testing correlation p^* from the previous section. This would guarantee that such a Bell inequality self-tests $|\Psi\rangle$. Geometrically, we wish to find a hyperplane tangent to the appropriate quantum correlation set precisely at p^*. We succeed at finding such a Bell inequality for the case where $|\Psi\rangle$ is the maximally entangled pair of qudits for any $d \geq 2$. Such a Bell inequality can be thought of as a generalization of CHSH to the qudit case. We note that this is not the first generalization of the CHSH inequality (or the CHSH game): a more natural algebraic generalization of the CHSH game over fields of order q was introduced by Buhrman and Massar [14], and studied by Bavarian and Shor [8]; another generalization was introduced by Tavakoli et al. and studied in the context of random access codes [94]. However, the self-testing properties of these generalizations are not known. On the other hand, we will understand completely the self-testing properties of our generalization: the inequality parametrized by the integer $d \geq 2$ self-tests the maximally entangled state of local dimension d. In Section 5.2.2, we also provide a conjecture for the general case: a family of Bell inequalities that self-tests any bipartite entangled state.

5.2.1 The Bell inequality

The family of Bell inequalities that we are about to introduce is over question sets $\mathcal{X} = \{0,1,2\}$ and $\mathcal{Y} = \{0,1,2,3\}$, and answer sets $\mathcal{A} = \mathcal{B} = \{0,..,d-1\}$ (where $d \geq 2$ corresponds to the local dimension). We introduce some notation. For a correlation $p \in \mathcal{C}_q^{3,4,d,d}$ and $m \in \{0,1,..\left\lfloor \frac{d}{2} \right\rfloor - 1\}$, define

$$[\mathrm{CHSH}_m]_p := \sum_{x,y \in \{0,1\}, a,b \in \{2m,2m+1\}} (-1)^{a \oplus b - xy} p(a,b|x,y)\,, \tag{5.16}$$

where $a \oplus b - xy$ is intended modulo 2. Note that for $m = 0$, this is the usual CHSH Bell functional. For $m > 0$ the form is the same, but the answers are in $\{2m, 2m+1\}$. In what follows, we will use the term "standard CHSH" to refer to the standard CHSH inequality or Bell functional on binary question and answer sets. This is to distinguish it from the new functionals we have just defined. We will also use the terms Bell operator and Bell functional interchangeably.

We can define a similar functional to (5.16) for questions $x \in \{0,2\}$ and $y \in \{2,3\}$ and answers in

$\{2m+1, 2m+2\}$. Here questions $x \in \{0,2\}$ and $y \in \{2,3\}$ take the role of the $\{0,1\}$ questions in (5.16). So, for convenience of notation define a relabelling map $f : \{0,2\} \to \{0,1\}$ to be such that $f(0) = 0, f(2) = 1$, and a relabelling map $g : \{2,3\} \to \{0,1\}$ to be such that $g(2) = 0$, $g(3) = 1$. Then, define

$$[\mathrm{CHSH}'_m]_p := \sum_{x\in\{0,2\},y\in\{2,3\},a,b\in\{2m+1,2m+2\}} (-1)^{a\oplus b - f(x)g(y)} p(a \bmod d, b \bmod d|x,y)\,.$$

From now onwards, we omit writing "mod d" for ease of notation, and the answers are intended mod d.

Denote by $\mathcal{C}$ and $\mathcal{C}'$ the sets

$$\mathcal{C} = \left\{ (a,b,x,y) : (x,y) \in \{0,1\}\times\{0,1\} \wedge (a,b) \notin \bigcup_{m=0}^{\lfloor \frac{d}{2}\rfloor -1} \{2m,2m+1\}\times\{2m,2m+1\} \right\}, \tag{5.17}$$

$$\mathcal{C}' = \left\{ (a,b,x,y) : (x,y) \in \{0,2\}\times\{2,3\} \wedge (a,b) \notin \bigcup_{m=0}^{\lfloor \frac{d}{2}\rfloor -1} \{2m+1,2m+2\}\times\{2m+1,2m+2\} \right\}. \tag{5.18}$$

Then, define the cross terms

$$[\mathrm{CROSS}]_p := \sum_{a,b,x,y:(a,b,x,y)\in\mathcal{C}} p(a,b|x,y),$$
$$[\mathrm{CROSS}']_p := \sum_{a,b,x,y:(a,b,x,y)\in\mathcal{C}'} p(a,b|x,y).$$

We are ready to define the family of Bell operators for our inequalities.

Definition 32 (The Bell operator)**.** *Let $d \geq 2 \in \mathbb{Z}$ and $\mathbb{1}_{\{d>2\}}$ and $\mathbb{1}_{\{d\ odd\}}$ be the indicator functions for the cases $d > 2$ and d odd respectively. Let $\delta > 0$ be a constant. For a correlation p, the Bell operator takes the form:*

$$[\mathcal{B}]_p := \sum_{m=0}^{\lfloor \frac{d}{2}\rfloor -1} [\mathrm{CHSH}_m]_p + \mathbb{1}_{\{d>2\}} \cdot \sum_{m=0}^{\lfloor \frac{d}{2}\rfloor -1} [\mathrm{CHSH}'_m]_p - \delta\cdot([\mathrm{CROSS}]_p + [\mathrm{CROSS}']_p)$$
$$+ \mathbb{1}_{\{d\ odd\}} \cdot \frac{\sqrt{2}}{2} \cdot \left(\sum_{x,y\in\{0,1\}} p(d-1,d-1|x,y) + \sum_{x\in\{0,2\},y\in\{2,3\}} p(0,0|x,y) \right) \tag{5.19}$$

Intuitively the terms CROSS and CROSS$'$ can be thought of as "penalty" terms: they are meant to enforce that any correlation maximizing the value of the Bell operator must put zero probability

mass on the cross terms from $\mathcal{C}$ and $\mathcal{C}'$. We will argue that it is enough to multiply these penalty terms by any arbitrarily small but positive constant δ to ensure that maximal violation is attained exclusively by the maximally entangled state. On the other hand, with a zero penalty, it is still the case that the corresponding Bell inequality can be maximally violated using a maximally entangled state, but we are unable to show that the self-testing result still holds true (i.e. the converse).

Theorem 16 (Classical bound)**.** *For any $d \geq 2$ and any $p \in \mathcal{C}_c^{3,4,d,d}$:*

$$[\mathcal{B}]_p \leq 2 \cdot (1 + \mathbb{1}_{\{d>2\}}) .$$

Proof. For $d = 2$ we recover the classical case of the standard CHSH inequality, so assume $d > 2$ from now on. Finding the best classical strategy is equivalent to finding the best deterministic strategy. Let $f_A : \{0,1,2\} \to \{0,..,d-1\}$ and $f_B : \{0,1,2,3\} \to \{0,..,d-1\}$ be functions specifying a deterministic strategy. Now, suppose $f_A(0) \in \{2k, 2k+1\}$, $f_A(1) \in \{2l, 2l+1\}$ and $f_A(2) \in \{2l', 2l'+1\}$.

- If $k = l$, It's easy to see that the best choice for $f_B(0)$ and $f_B(1)$ is to have also $f_B(0), f_B(1) \in \{2k, 2k+1\}$ and get a contribution of at most 2 (this is from the standard CHSH classical bound)
- if $k \neq l$, it's also easy to see that the best choice for $f_B(0)$ and $f_B(1)$ is to have one of three possibilities: $f_B(0), f_B(1) \in \{2k, 2k+1\}$; $f_B(0), f_B(1) \in \{2l, 2l+1\}$; or one in $\{2k, 2k+1\}$ and the other in $\{2l, 2l+1\}$. They all achieve a contribution of at most 2.

Similarly, the best possible choice for $f_B(2)$ and $f_B(3)$ gives a contribution of 2. This yields the desired bound. □

We turn to quantum correlations. We have the following two theorems:

Theorem 17 (Quantum bound)**.** *For any d even and any $p \in \mathcal{C}_q^{3,4,d,d}$:*

$$[\mathcal{B}]_p \leq 2\sqrt{2} \cdot (1 + \mathbb{1}_{\{d>2\}}) . \tag{5.20}$$

Theorem 18 (Exact self-testing)**.** *For any $d \geq 2$, there is a unique correlation which achieves the quantum bound of $\mathcal{B}$, and it self-tests the state $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$.*

5.2.1.1 Proof overview

At a high level, the proof of Theorems 17 and 18 goes through the following steps:

(i) The correlation from [23] (in the maximally entangled case), achieves the RHS of (5.20) (Lemma 38);

(ii) Any correlation achieving the maximal quantum value of the Bell operator must have zero probability mass on the cross terms. This is proved by starting from a correlation which achieves the maximum but has non-zero cross terms, and modifying this into a strategy for qubit CHSH which achieves a value strictly higher than $2\sqrt{2}$, which is a contradiction. (This is the content of Lemma 39);

(iii) Having zero cross-terms forces the correlations to have the block-diagonal form of [23]. The 2×2 blocks are across pairs of answers $\{2m, 2m+1\}$ for questions $x, y \in \{0,1\}$ and across pairs of answers $\{2m+1, 2m+2\}$ for questions $x \in \{0,2\}, y \in \{2,3\}$ (Lemma 40);

(iv) Finally, the freedom in the value of the weights of the blocks is fixed by the requirement that the block-diagonal structure is both over pairs of answers $\{2m, 2m+1\}$, for $x, y \in \{0,1\}$, and also over pairs of answers $\{2m+1, 2m+2\}$, for $x \in \{0,2\}, y \in \{2,3\}$, and these two subsets of questions have in common the question $x = 0$.

5.2.1.2 The ideal correlation

We will now describe ideal correlations achieving the quantum bound of (5.20). For a single-qubit observable A, we denote by $(A)_m$ the observable defined with respect to the basis $(|2m\rangle, |2m+1\rangle)$. For example, $(\sigma_Z)_m = |2m\rangle\langle 2m| - |2m+1\rangle\langle 2m+1|$. Similarly, we denote by $(A)'_m$ the observable defined with respect to the basis $(|2m+1\rangle, |2m+2\rangle)$.

Lemma 38 (Ideal correlation from [23] achieving the quantum bound)**.** *The correlation $p^* \in \mathcal{C}_q^{3,4,d,d}$ specified by the following quantum strategy $(|\Psi\rangle, \{\Pi^a_{A_x}\}_a, \{\Pi^b_{B_y}\}_b)$ achieves the RHS of* (5.20)*:*

- $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$
- *For* $m = 0, .., \left\lfloor \frac{d}{2} \right\rfloor - 1$*:*
  - $\Pi^{2m}_{A_0}, \Pi^{2m+1}_{A_0}$ *are the projectors respectively onto the* $+1, -1$ *eigenspaces of* $(\sigma_Z)_m$*. (in other words, the measurement for* $x = 0$ *is in the computational basis);*

- $\Pi_{A_1}^{2m}$, $\Pi_{A_1}^{2m+1}$ *onto the* $+1,-1$ *eigenspaces of* $(\sigma_X)_m$. *If* d *is odd,* $\Pi_{A_1}^{d-1} = |d-1\rangle\langle d-1|$
- $\Pi_{A_2}^{2m+1}$, $\Pi_{A_2}^{2m+2}$ *onto the* $+1,-1$ *eigenspaces of* $(\sigma_X)'_m$. *If* d *is odd,* $\Pi_{A_2}^{0} = |0\rangle\langle 0|$.

• *For* $m = 0,..,\left\lfloor \frac{d}{2} \right\rfloor - 1$*:*

- *For* $y \in \{0,1\}$, $\Pi_{B_y}^{2m}$, $\Pi_{B_y}^{2m+1}$ *are the projectors respectively onto the* $+1,-1$ *eigenspaces of* $(\frac{\sigma_Z+(-1)^y\sigma_X}{\sqrt{2}})_m$. *If* d *is odd,* $\Pi_{B_y}^{d-1} = |d-1\rangle\langle d-1|$*;*
- *For* $y \in \{2,3\}$, $\Pi_{B_y}^{2m+1}$, $\Pi_{B_y}^{2m+2}$ *onto the* $+1,-1$ *eigenspaces of* $(\frac{\sigma_Z+(-1)^y\sigma_X}{\sqrt{2}})'_m$. *If* d *is odd,* $\Pi_{B_y}^{0} = |0\rangle\langle 0|$.

Proof. This is a straightforward check. □

5.2.1.3 Proof of Theorems 17 and 18

Lemma 39 (Zero mass on the cross terms)**.** *Let* $p \in \mathcal{C}_q^{3,4,d,d}$ *be a quantum correlation achieving maximal quantum value of* $\mathcal{B}$*. Then,* $p(a,b|x,y) = 0\ \forall (a,b,x,y) \in \mathcal{C} \cup \mathcal{C}'$*, where* $\mathcal{C}$ *and* $\mathcal{C}'$ *are as in equations* (5.17) *and* (5.18)*.*

This establishes that any correlation maximally violating the Bell inequality must have the same block-diagonal form of the self-testing correlation from Lemma 38.

Proof. We argue first for the case of d even. We will show that any correlation achieving maximal value of $\mathcal{B}$ must have $p(a,b|x,y) = 0\ \ \forall (a,b,x,y) \in \mathcal{C} \cup \mathcal{C}'$. Suppose for a contradiction that a correlation $p \in \mathcal{C}_q^{3,4,d,d}$ achieves the maximal value of $\mathcal{B}$ and $p(a,b|x,y) = \gamma > 0$ for some $(a,b,x,y) \in \mathcal{C} \cup \mathcal{C}'$. In order to compensate for the negative contribution due to the presence of the cross terms in (5.19) (which are multiplied by an arbitrary small but positive constant δ), it must be the case that either $\sum_{m=0}^{\frac{d}{2}-1}[\mathrm{CHSH}_m]_p > 2\sqrt{2}$ or $\sum_{m=0}^{\frac{d}{2}-1}[\mathrm{CHSH}'_m]_p > 2\sqrt{2}$ (since we know from Lemma 38 that the maximal value of $\mathcal{B}$ is at least $2 \cdot 2\sqrt{2}$.). Assume the former (the other case being similar).

Let $S = (|\psi\rangle, \Pi_{A_x}^a, \Pi_{B_y}^b)$ be a quantum strategy producing correlation p. We will use this to construct a correlation $\tilde{p} \in \mathcal{C}_q^{2,2,2,2}$ that achieves a value of CHSH greater than $2\sqrt{2}$, which would be a contradiction. This is achieved by starting from strategy S and mapping each pair of answers $(2k, 2k+1)$ in $\{2,..,d-1\}$ to either their parity or the opposite of their parity, i.e either $(2k,2k+1) \mapsto (0,1)$ or $(2k,2k+1) \mapsto (1,0)$. More precisely, for $\mathbf{o} \in \{0,1\}^{\frac{d}{2}-1}$ let

$\mathbf{o}[m]$ denote the mth bit of $\mathbf{o}$, and define a new quantum strategy for standard CHSH $S^{(\mathbf{o})} = (|\psi\rangle, \{\tilde{\Pi}^a_{A_x}\}_{a,x\in\{0,1\}}, \{\tilde{\Pi}^b_{B_y}\}_{b,y\in\{0,1\}})$ on the same state $|\psi\rangle$, with projectors, for $x, y \in \{0,1\}$,

$$\tilde{\Pi}^0_{A_x} = \Pi^0_{A_x} + \sum_{m=1}^{\frac{d}{2}-1} \Pi^{2m+\mathbf{o}[m]}_{A_x} \qquad \tilde{\Pi}^1_{A_x} = \Pi^1_{A_x} + \sum_{m=1}^{\frac{d}{2}-1} \Pi^{2m+1-\mathbf{o}[m]}_{A_x}$$

$$\tilde{\Pi}^0_{B_y} = \Pi^0_{B_y} + \sum_{m=1}^{\frac{d}{2}-1} \Pi^{2m+\mathbf{o}[m]}_{B_y} \qquad \tilde{\Pi}^1_{B_y} = \Pi^1_{B_y} + \sum_{m=1}^{\frac{d}{2}-1} \Pi^{2m+1-\mathbf{o}[m]}_{B_y}$$

Let $\tilde{p}^{(\mathbf{o})}$ be the resulting correlation. Now, let $[\text{CHSH}]_{\tilde{p}^{(\mathbf{o})}}$ be the CHSH value of correlation $\tilde{p}^{(\mathbf{o})}$. Since CHSH is an XOR game (i.e. only the xor of the answers matters), it's easy to see that for any $\mathbf{o} \in \{0,1\}^{\frac{d}{2}-1}$

$$[\text{CHSH}]_{\tilde{p}^{(\mathbf{o})}} = \sum_{m=0}^{\frac{d}{2}-1} [\text{CHSH}_m]_p + C\,,$$

where C is a (possibly negative) contribution which comes from the cross terms of the form $\langle\psi| \Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle$ for $(a,b,x,y) \in \mathcal{C}$. However, there exists a choice of $\mathbf{o} \in \{0,1\}^{\frac{d}{2}-1}$ such that $C \geq 0$. In fact, notice that the contributions to C coming from cross terms involving $(2m, 2m+1)$ when one chooses $\mathbf{o}[m] = 0$ or $\mathbf{o}[m] = 1$ (and keeps the other choices fixed) are the negative of each other. Hence at least one of the two choices gives a non-negative contribution. Then, pick $\mathbf{o} \in \{0,1\}^{\frac{d}{2}-1}$ as follows: for $m = 1, .., \frac{d}{2}-1$, in this order, choose a value of $\mathbf{o}[m]$ for which the contribution from cross terms involving pairs $(2m, 2m+1)$ and $(2m', 2m'+1)$ for $m' < m$ is non-negative. This gives $C \geq 0$.

So, for this choice of $\mathbf{o}$, one gets $[\text{CHSH}]_{\tilde{p}^{(\mathbf{o})}} > 2\sqrt{2}$, which is the desired contradiction.

The case of d odd is similar but requires slightly more effort. Suppose $p \in \mathcal{C}_q^{3,4,d,d}$ achieves the maximal value of $\mathcal{B}$ and $p(a,b|x,y) = \gamma > 0$ for some $(a,b,x,y) \in \mathcal{C} \cup \mathcal{C}'$. Then it must be the case that either $\sum_{m=0}^{\frac{d}{2}-1} [\text{CHSH}_m]_p + \frac{\sqrt{2}}{2} \cdot \sum_{x,y\in\{0,1\}} p(d-1, d-1|x,y) > 2\sqrt{2}$ or $\sum_{m=0}^{\frac{d}{2}-1} [\text{CHSH}'_m]_p + \frac{\sqrt{2}}{2} \cdot \sum_{x\in\{0,2\},y\in\{2,3\}} p(0,0|x,y) > 2\sqrt{2}$. Suppose the former (the latter case being similar). Let $S = (|\psi\rangle, \Pi^a_{A_x}, \Pi^b_{B_y})$ be a quantum strategy producing correlation p. For a string $\mathbf{o} \in \{0,1\}^{\frac{d}{2}-1}$, we construct the following strategy for CHSH $S^{(\mathbf{o})} = (|\tilde{\psi}\rangle, \{\tilde{\Pi}^a_{A_x}\}_{a,x\in\{0,1\}}, \{\tilde{\Pi}^b_{B_y}\}_{b,y\in\{0,1\}})$: intuitively, the two parties share the original state tensored with an EPR pair. They map outcomes $\{0, .., d-2\}$ to outcomes in $\{0,1\}$ (similarly as before). If one sees outcome $d-1$, they measure the shared EPR pair with an appropriate ideal CHSH measurement. More precisely, let $\{P^a_{A_x}\}_{a,x\in\{0,1\}}, \{P^b_{B_y}\}_{b,y\in\{0,1\}}$ be the ideal CHSH qubit

measurements. Then, $|\tilde{\psi}\rangle = |\psi\rangle \otimes |\text{EPR}\rangle$, and

$$\tilde{\Pi}^0_{A_x} = [\Pi^0_{A_x} + \sum_{m=1}^{\lfloor \frac{d}{2} \rfloor - 1} \Pi^{2m+\mathbf{o}[m]}_{A_x}] \otimes I + \Pi^{d-1}_{A_x} \otimes P^0_{A_x},$$

$$\tilde{\Pi}^1_{A_x} = [\Pi^1_{A_x} + \sum_{m=1}^{\lfloor \frac{d}{2} \rfloor - 1} \Pi^{2m+1-\mathbf{o}[m]}_{A_x}] \otimes I + \Pi^{d-1}_{A_x} \otimes P^1_{A_x},$$

$$\tilde{\Pi}^0_{B_y} = [\Pi^0_{B_y} + \sum_{m=1}^{\lfloor \frac{d}{2} \rfloor - 1} \Pi^{2m+\mathbf{o}[m]}_{B_y}] \otimes I + \Pi^{d-1}_{B_y} \otimes P^0_{B_y},$$

$$\tilde{\Pi}^1_{B_y} = [\Pi^1_{B_y} + \sum_{m=1}^{\lfloor \frac{d}{2} \rfloor - 1} \Pi^{2m+1-\mathbf{o}[m]}_{B_y}] \otimes I + \Pi^{d-1}_{B_y} \otimes P^1_{B_y}.$$

One can check, then, that with the appropriate choice of $\mathbf{o}$ (chosen similarly to the d even case), this gives a strategy for CHSH which achieves a value strictly greater than $2\sqrt{2}$.

□

The following lemma establishes that if a correlation p has zero cross-terms, then this implies that the restriction of p to the subset of questions $(x, y) \in \{0,1\}^2$ and to answers $a, b \in \{2m, 2m+1\}$ is still a correlation (multiplied by some weight). Likewise for the restriction to the subset of questions $(x, y) \in \{0,2\} \times \{2,3\}$ and to answers $a, b \in \{2m+1, 2m+2\}$.

Lemma 40. *Any correlation $p \in \mathcal{C}_q^{3,4,d,d}$ with zero cross-terms (i.e of the form of Lemma 39), induced by some strategy $\left(|\psi\rangle, \{\Pi^a_{A_x}\}_a, \{\Pi^b_{B_y}\}_b\right)$, satisfies the following:*

- *If d is even, for each $m = 0, .., \frac{d}{2} - 1$, there exist weights $w_m, w'_m \geq 0$ with $\sum_m w_m = 1$, $\sum_m w'_m = 1$ and correlations $p_m, p'_m \in \mathcal{C}_q^{2,2,2,2}$ (with questions in $\{0,1\}^2$ and $\{0,2\} \times \{2,3\}$ respectively, and answers in $\{0,1\}$) such that $\forall m$, $\forall a, b \in \{2m, 2m+1\}, x, y \in \{0,1\}$:*

$$p(a, b|x, y) = w_m \cdot p_m(a \mod 2, b \mod 2|x, y) = \langle\psi| \Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle \tag{5.21}$$

  and $\forall m$, $\forall a, b \in \{2m+1, 2m+2\}, x \in \{0,2\}, y \in \{2,3\}$:

$$p(a, b|x, y) = w'_m \cdot p'_m(a \mod 2, b \mod 2|x, y) = \langle\psi| \Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle$$

- *If d is odd, the analogous statement holds, except that the weights w_m, w'_m are such that $\sum_m w_m + p(d-1, d-1|0,0) = \sum_m w'_m + p(0,0|2,2) = 1$, AND*
  - *$p(d-1, d-1|x, y) = p(d-1, d-1|x', y')$ $\forall x, y, x'y' \in \{0,1\}$*

– $p(0,0|x,y) = p(0,0|x',y')\ \forall x,x' \in \{0,2\}, y,y' \in \{2,3\}$

Proof. Let $p \in \mathcal{C}_q^{3,4,d,d}$ be of the form of Lemma 39, and let $(|\psi\rangle, \{\Pi^a_{A_x}\}, \{\Pi^b_{B_y}\})$, be a strategy reproducing p. Then, for $m = 0, .., \frac{d}{2} - 1$ define:

(i) for $x,y \in \{0,1\}$, $A_x^{(m)} = \Pi_{A_x}^{2m} - \Pi_{A_x}^{2m+1}$ and $B_y^{(m)} = \Pi_{B_y}^{2m} - \Pi_{B_y}^{2m+1}$

(ii) for $x \in \{0,2\}, y \in \{2,3\}$, $A_x'^{(m)} = \Pi_{A_x}^{2m+1} - \Pi_{A_x}^{2m+2}$ and $B_y'^{(m)} = \Pi_{B_y}^{2m+1} - \Pi_{B_y}^{2m+2}$

Define the subspaces $\mathcal{U}_m = \text{Range}(A_0^{(m)}) + \text{Range}(A_1^{(m)})$ and $\mathcal{V}_m = \text{Range}(B_0^{(m)}) + \text{Range}(B_1^{(m)})$, and let $\mathbb{1}_{\mathcal{U}_m}$ and $\mathbb{1}_{\mathcal{V}_m}$ be projections onto these subspaces. Let $|\psi_m\rangle := \mathbb{1}_{\mathcal{U}_m}\mathbb{1}_{\mathcal{V}_m}|\psi\rangle$ We will check that $\mathbb{1}_{\mathcal{U}_m}|\psi\rangle = \mathbb{1}_{\text{Range}(A_0^{(m)})}|\psi\rangle = \mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle = \mathbb{1}_{\mathcal{V}_m}|\psi\rangle = |\psi_m\rangle$. We compute

$$\begin{aligned}
\mathbb{1}_{\text{Range}(A_0^{(m)})}|\psi\rangle &= \left(\Pi_{A_0}^{2m} + \Pi_{A_0}^{2m+1}\right)|\psi\rangle \\
&= \left(\Pi_{A_0}^{2m} + \Pi_{A_0}^{2m+1}\right)\sum_{l=0}^{d-1}\Pi_{B_0}^{l}|\psi\rangle \\
&= \left(\Pi_{A_0}^{2m} + \Pi_{A_0}^{2m+1}\right)\left(\Pi_{B_0}^{2m} + \Pi_{B_0}^{2m+1}\right)|\psi\rangle \qquad (5.22)\\
&= \mathbb{1}_{\text{Range}(A_0^{(m)})}\mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle\,, \qquad (5.23)
\end{aligned}$$

where the third line follows from the hypothesis that the correlation has the form of Lemma 39. The same calculation starting from $\mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle$ gives $\mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle = \mathbb{1}_{\text{Range}(A_0^{(m)})}\mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle$, which, together with (5.23), implies $\mathbb{1}_{\text{Range}(A_0^{(m)})}|\psi\rangle = \mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle$. With similar calculations, we also deduce $\mathbb{1}_{\text{Range}(A_1^{(m)})}|\psi\rangle = \mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle$, which implies $\mathbb{1}_{\text{Range}(A_0^{(m)})}|\psi\rangle = \mathbb{1}_{\text{Range}(A_1^{(m)})}|\psi\rangle$, and hence $\mathbb{1}_{\mathcal{U}_m}|\psi\rangle = \mathbb{1}_{\text{Range}(A_0^{(m)})}|\psi\rangle$. Similarly $\mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle = \mathbb{1}_{\text{Range}(B_1^{(m)})}|\psi\rangle$, and hence $\mathbb{1}_{\mathcal{V}_m}|\psi\rangle = \mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle$. Altogether, we have deduced that

$$\mathbb{1}_{\mathcal{U}_m}|\psi\rangle = \mathbb{1}_{\text{Range}(A_0^{(m)})}|\psi\rangle = \mathbb{1}_{\text{Range}(B_0^{(m)})}|\psi\rangle = \mathbb{1}_{\mathcal{V}_m}|\psi\rangle = |\psi_m\rangle\ .$$

Finally, set $w_m = \||\psi_m\rangle\|^2$ to get the desired weights, and take the correlations p_m as in (5.21). We argue similarly for the weights w'_m and the correlations p'_m. A very similar argument yields the conclusion for the case of odd d.

□

Corollary 5. *Any correlation $p \in \mathcal{C}_q^{3,4,d,d}$ with zero cross-terms (i.e. of the form of Lemma 39) satisfies the following:*

- *If d is even, there exist weights $w_m, w'_m \geq 0$, $m = 0, .., \frac{d}{2} - 1$, with $\sum_m w_m = 1$, $\sum_m w'_m = 1$, such that, for all m,*

$$[\mathrm{CHSH}_m]_p \leq w_m \cdot 2\sqrt{2}$$

and

$$[\mathrm{CHSH}'_m]_p \leq w'_m \cdot 2\sqrt{2}$$

- *If d is odd, the analogous statement holds, except that the weights w_m, w'_m are such that $\sum_m w_m + p(d,d|0,0) = 1$, $\sum_m w'_m + p(0,0|2,2) = 1$.*

Proof. This follows immediately from Lemma 40. □

Proof of Theorems 17 and 18. Assume $d > 2$, as the $d = 2$ case corresponds to standard CHSH. We start with d even (the odd case being similar). Let $p \in \mathcal{C}_q^{3,4,d,d}$ be a correlation that achieves the maximal quantum value of $\mathcal{B}$. By Lemma 39, p must have zero cross-terms. Then, from Lemma 40, we deduce, for $m = 0, .., \frac{d}{2} - 1$, the existence of weights w_m, w'_m and correlations p_m, p'_m satisfying the statement of the Lemma. This implies

$$\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}_m]_p = \sum_{m=0}^{\frac{d}{2}-1} w_m \cdot [\mathrm{CHSH}]_{p_m} \leq 2\sqrt{2}\,,$$

where we have bounded each term with the standard CHSH bound. Similarly, we also get $\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}'_m]_p \leq 2\sqrt{2}$, which implies the desired upper bound of Theorem 17.

Such upper bound is achieved if and only if $[\mathrm{CHSH}]_{p_m} = w_m \cdot 2\sqrt{2}$ for all m, and $[\mathrm{CHSH}'_m]_p = w'_m \cdot 2\sqrt{2}$ for all m. This is if and only if:

- for all m, $w_m = 0$ OR p_m is the ideal qubit CHSH correlation, AND
- for all m, $w'_m = 0$ OR p'_m is the ideal qubit CHSH correlation

We want to argue that the only way that this can happen is if the weights are all equal (and non-zero). Once we have shown this, we notice that we have specified the correlation p completely for the two subsets of questions $x, y \in \{0,1\}$ and $x \in \{0,2\}, y \in \{2,3\}$. From [23], we know this is enough to uniquely determine the self-testing correlation for the maximally entangled state of local dimension d presented in [23] (and in Lemma 38), and we thus deduce that maximal violation of the Bell inequality self-tests $|\Psi\rangle$.

Let $(|\psi\rangle, \{\Pi^a_{A_x}\}_a, \{\Pi^b_{B_y}\}_b$ be a quantum strategy for p (which achieves the upper bound). Then, by what we have argued above, for all m we have $\|\Pi^{2m+1}_{A_0}|\psi\rangle\|^2 = w_m \cdot \frac{1}{2}$, and this holds both when $w_m \neq 0$ (and p_m is the ideal qubit CHSH correlation) and when $w_m = 0$. Likewise, we have that $\|\Pi^{2m+1}_{A_0}|\psi\rangle\|^2 = w'_m \cdot \frac{1}{2}$. And similarly $\|\Pi^{2m}_{A_0}|\psi\rangle\|^2 = w_m \cdot \frac{1}{2}$ and $\|\Pi^{2m}_{A_0}|\psi\rangle\|^2 = w'_{m-1} \cdot \frac{1}{2}$. Clearly this, together with the constraint $\sum_m w_m = \sum_m w'_m = 1$, implies $w_m = w'_m = \frac{2}{d}\ \forall m$.

The proof is similar for the case of d odd, where we instead deduce $w_m = w'_m = \frac{2}{d}\ \forall m$ (there are $\frac{d-1}{2}$ values of m) and $p(d-1, d-1|x,y) = p(0,0|x',y') = \frac{1}{d}\ \forall x,y \in \{0,1\}, x' \in \{0,2\}, y' \in \{2,3\}$. □

A robust version of the self-testing result *via the correlations* of [23] was shown in [25], where, informally, the authors prove that a strategy producing a correlation that is ϵ-close to the ideal one, must be $O(d^3\epsilon^{\frac{1}{4}})$-close (according to some measures of distance) to the ideal strategy from Lemma 38. However, this does not trivially translate to a robust self-test *via our Bell inequality*, for which we require that a *close-to-maximal violation* certifies a close-to-ideal strategy. Since translating the exact analysis to a robust analysis is not particularly illuminating, we leave the details to the appendix. For the robust self-testing theorem via our Bell inequality, refer to Theorem 36 in the Appendix.

5.2.2 Generalizing the tilted CHSH inequality (a conjecture)

Let $I_\alpha = \sqrt{8 + 2\alpha^2}$ be the maximal quantum violation of the tilted CHSH inequality, for coefficient α. The family of candidate Bell inequalities which we will describe is a very natural generalization of the Bell inequality from the previous section to the tilted case. We introduce some notation. For a correlation $p \in \mathcal{C}_q^{3,4,d,d}$, define

$$[\text{tCHSH}_m(\alpha)]_p := \ \alpha[p(a = 2m|x = 0) - p(a = 2m+1|x = 0)] + [\text{CHSH}_m]_p\,,$$

where $[\text{CHSH}_m]_p$ was defined earlier. This can be thought of as a tilted CHSH Bell operator restricted to answers in $\{2m, 2m+1\}$. Note that the above involves only questions $x, y \in \{0,1\}$. We can define a similar term for questions in $x \in \{0,2\}$ and $y \in \{2,3\}$ and answers in $\{2m+1, 2m+2\}$. Let

$$[\text{tCHSH}'_m(\alpha)]_p := \ \alpha[p(a = 2m+1|x = 0) - p(a = 2m+2|x = 0)] + [\text{CHSH}'_m]_p\,.$$

The sets $\mathcal{C}$ and $\mathcal{C}'$ of questions and answers corresponding to cross terms are defined as in the previous section. Then our candidate family of Bell operators generalizing the family of tilted CHSH inequalities is the following:

Definition 33 (The family of Bell operators)**.** *Each inequality in the family is specified by:*

(i) $0 < c_i < 1 \in \mathbb{R}$, $i = 0, .., d-1$, *with* $\sum_{i=0}^{d-1} c_i^2 = 1$,

(ii) $d \geq 2 \in \mathbb{N}$

Let $\theta_m = \arctan \frac{c_{2m+1}}{c_{2m}}$, $\alpha_m \equiv \alpha_m(\theta_m) \in [0,2)$ *be defined by* $\sin 2\theta_m = \sqrt{\frac{4-\alpha_m^2}{4+\alpha_m^2}}$, $\theta'_m = \arctan \frac{c_{2m+2}}{c_{2m+1}}$, $\alpha'_m \equiv \alpha'_m(\theta'_m) \in [0,2)$ *defined by* $\sin 2\theta'_m = \sqrt{\frac{4-\alpha_m'^2}{4+\alpha_m'^2}}$. *Let* $\delta > 0$ *be a constant. For a correlation* $p \in \mathcal{C}_q^{3,4,d,d}$, *the Bell operator takes the form:*

$$\begin{aligned}[t\mathcal{B}(c_0, .., c_{d-1})]_p := & \sum_{m=0}^{\lfloor \frac{d}{2} \rfloor - 1} \frac{1}{I_{\alpha_m}} [\text{tCHSH}_m(\alpha_m)]_p + \mathbb{1}_{\{d>2\}} \cdot \sum_{m=0}^{\lfloor \frac{d}{2} \rfloor - 1} \frac{1}{I_{\alpha'_m}} [\text{tCHSH}'_m(\alpha'_m)]_p \\ & - \delta \cdot ([\text{CROSS}]_p + [\text{CROSS}']_p) \\ & + \mathbb{1}_{\{d \text{ odd}\}} \cdot \frac{1}{4} \cdot \left(\sum_{x,y \in \{0,1\}} p(d-1, d-1|x,y) + \sum_{x \in \{0,2\}, y \in \{2,3\}} p(0,0|x,y) \right) . \end{aligned} \tag{5.24}$$

Note that to put the Bell operator for the maximally entangled case in this form one just needs to divide (5.19) by $2\sqrt{2}$.

Conjecture 1 (Quantum bound and self-testing)**.** *For any* d *even and any* $p \in \mathcal{C}_q^{3,4,d,d}$:

$$[t\mathcal{B}(c_0, .., c_{d-1})]_p \leq 1 + \mathbb{1}_{\{d>2\}} .$$

Moreover, there is a unique quantum correlation achieving the bound, and it self-tests the state $|\Psi\rangle = \sum_{i=0}^{d-1} c_i |ii\rangle$.

The lack of symmetry in the tilted case seems to make the analysis surprisingly less straightforward, and the arguments we employed in the maximally entangled case do not directly carry over.

An open question that applies to both the maximally entangled and the tilted Bell operators is to determine if cross terms are necessary for the self-testing property to hold true (i.e. whether, in (5.19) and (5.24), $\delta > 0$ is necessary or $\delta = 0$ suffices).

5.3 Self-testing multipartite states through projections onto two systems

In this section, we move to the multipartite setting. In contrast to the bipartite setting, only a handful of self-testing results are known in the multipartite setting, but we expect the question of self-testing multipartite states to become increasingly relevant as quantum cryptographic applications that involve a network of quantum parties become viable.

Here, we significantly expand the class of self-testable multipartite states. More precisely, in Subsection 5.3.2.1 we show that all multipartite partially entangled GHZ (qubit) states can be self-tested with two measurements per party. Then, we make use of this result as a building block to extend self-testing to all multipartite entangled Schmidt-decomposable qudit states, of any local dimension d and for any number of parties. We do so with a correlation on question sets of size 3 and answer sets of size 2 (except one party has 4 questions). To the best of our knowledge, this is the first self-test for multipartite states of qudits for $d > 2$.

5.3.1 Preliminaries

We have to introduce some additional notation for the multipartite case. There are now N non-communicating parties sharing an N-partite state $|\psi\rangle$. Each party i, on its share of this state, can perform one of several projective measurements $\{M_{x_i,i}^{a_i}\}_{a_i}$, labelled by $x_i \in \mathcal{X}_i$, with possible outcomes $a_i \in \mathcal{A}_i$. Here $\mathcal{X}_i$ and $\mathcal{A}_i$ stand for finite alphabets of possible questions and answers for party i. We refer to $|\psi\rangle$, together with $\{M_{x_i,i}^{a_i}\}_{a_i}$ as an *$N-$partite quantum strategy*. The *$N-$partite correlation* that it induces is $\{p(a_1,\ldots,a_N|x_1,\ldots,x_N) : a_i \in \mathcal{A}_i\}_{x_i\in\mathcal{X}_i}$, where

$$p(a_1,\ldots,a_N|x_1,\ldots,x_N) = \langle\psi|M_{x_1,1}^{a_1}\otimes\ldots\otimes M_{x_N,N}^{a_N}|\psi\rangle$$

is the probability of obtaining answers $a_1,\ldots,a_N$ upon receiving questions $x_1,\ldots,x_N$[1]. As in the bipartite case, it is often convenient to describe correlations using observables with eigenvalues ± 1. The definition of self-testing for the multipartite case is the natural extension of the definition for the bipartite case.

Definition 34 (Self-testing, multipartite case)**.** *We say that a correlation $\{p(a_1,\ldots,a_N|x_1,\ldots,x_N) : a_i \in \mathcal{A}_i\}_{x_i\in\mathcal{X}_i}$ self-tests the state $|\Psi\rangle$ and measurements $\{\tilde{M}_{x_i,i}^{a_i}\}_{a_i}$, $i = 1,\ldots,N$, if for any state and measurements $|\psi\rangle$ and $\{M_{x_i,i}^{a_i}\}_{a_i}$, $i = 1,\ldots,N$, reproducing the correlation, there exists a local isometry $\Phi = \Phi_1\otimes\ldots\otimes\Phi_N$ and an auxiliary*

[1] We take the parties' measurements to be projective, invoking Naimark's dilation theorem. We take the joint state to be pure for ease of exposition, but we emphasize that all of our proofs hold analogously starting from a joint mixed state.

state $|extra\rangle$ *such that*

$$\Phi(M_{x_1,1}^{a_1} \otimes \ldots \otimes M_{x_N,N}^{a_N} |\psi\rangle) = (\tilde{M}_{x_1,1}^{a_1} \otimes \ldots \otimes \tilde{M}_{x_N,N}^{a_N} |\psi'\rangle) \otimes |extra\rangle \ .$$

In some cases the existence of an isometry obeying (34) can be proven solely from the maximal violation of some Bell inequality. For instance, as we have seen several times by now, all two-qubit pure entangled states can be self-tested with a one-parameter class of tilted CHSH Bell inequalities [7] given by

$$\alpha\langle A_0\rangle + \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq 2 + \alpha \, ,$$

where $\alpha \geq 0$ and A_i and B_i are observables with outcomes ± 1 measured by the parties. As will be using it later on, Let us recall the following result, which is a step in the proof of the self-testing theorem for tilted CHSH.

Lemma 41 ([7])**.** *Suppose a bipartite state* $|\psi\rangle$ *and dichotomic observables* A_i *and* B_i *achieve the maximal quantum violation of the tilted CHSH inequality (5.3.1)* $\sqrt{8+2\alpha^2}$*, for some* α*. Let* $\theta, \mu \in (0, \pi/2)$ *be such that* $\sin 2\theta = \sqrt{(4-\alpha^2)/(4+\alpha^2)}$ *and* $\mu = \arctan \sin 2\theta$*. Let* $Z_A = A_0$*,* $X_A = A_1$*. Let* Z_B^* *and* X_B^* *be respectively* $(B_0 + B_1)/2\cos\mu$ *and* $(B_0 - B_1)/2\sin\mu$*, but with all zero eigenvalues replaced by one, and define* $Z_B = Z_B^*|Z_B^*|^{-1}$ *and* $X_B = X_B^*|X_B^*|^{-1}$*. Then, we have*

$$Z_A |\psi\rangle = Z_B |\psi\rangle \, ,$$
$$\cos\theta X_A(\mathbb{1} - Z_A) |\psi\rangle = \sin\theta X_B(\mathbb{1} + Z_A) |\psi\rangle \, .$$

Moreover, there exists a local isometry Φ *such that* $\Phi(A_i \otimes B_j |\psi\rangle) = |extra\rangle \otimes (\tilde{A}_i \otimes \tilde{B}_j) |\psi_\theta\rangle$*, where* $|\psi_\theta\rangle = \cos\theta |00\rangle + \sin\theta |11\rangle$*, and* $\tilde{A}_0 = \sigma_Z$*,* $\tilde{A}_1 = \sigma_X$*, and* $\tilde{B}_{0/1} = \cos\mu\sigma_z \pm \sin\mu\sigma_X$*.*

A typical construction of the isometry Φ is the one encoding the SWAP gate, as illustrated in Fig. 5.4.

5.3.2 Self-testing N-partite states by projecting onto two parties

Our aim in this paper is to exploit the above result to develop methods for self-testing multipartite entangled quantum states. Given an N-partite entangled state $|\psi\rangle$, the idea is that $N-2$ chosen parties perform local measurements on their shares of $|\psi\rangle$ and the remaining two parties check whether the projected state they share violates maximally (5.3.1) for the appropriate α (we can think of this as a sub-test). This procedure is repeated for various subsets of $N-2$ parties until the correlations imposed are sufficient to characterize the state $|\psi\rangle$. Our approach is inspired by Ref.

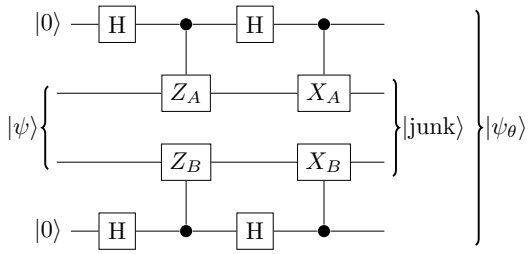


Figure 5.4: Example of a circuit that takes as input a state $|\psi\rangle$ satisfying (41-41), adds two ancillas, each in $|0\rangle$, and outputs the state $|\psi_\theta\rangle$ in tensor product with an auxiliary state $|extra\rangle$. Here H is the usual Hadamard gate.

[101], which shows that any state in the class $(|100\rangle + |101\rangle + \alpha\,|001\rangle)/\sqrt{2+\alpha^2}$, containing the three-qubit W state, can be self-tested in this way. We will show that this approach can be generalized in order to self-test new (and old) classes of multipartite states. The main challenge is to show that all the sub-tests of different pairs of parties are compatible. To be more precise, for a generic state there will always be a party which will be involved in several different sub-tests and, in principle, will be required to use different measurements to pass the different tests. Consequently, isometries (Fig. 5.4) corresponding to different sub-tests are in principle constructed from different observables. However, a single isometry is required in order to self-test the global state. Overcoming the problem of building a single isometry from several different ones is the key step to achieve a valid self-test for multipartite states. For states that exhibit certain symmetries, this can be done efficiently with few measurements. We leave for future work the exploration for states that do not have any particular symmetry.

In the N-partite scenario, parties will be denoted by numbers from 1 to N and measurement observables by capital letters with a superscript denoting the party. For a two-outcome observable W, we denote by $W^{(\pm)} = (\mathbb{I} \pm W)/2$ the projectors onto the ± 1 eigenspaces. We use the notation $\lfloor a \rfloor$ to denote the biggest integer n such that $n \leq a$, while $\lceil a \rceil$ is the smallest n such that $n \geq a$.

5.3.2.1 All multipartite entangled qudit Schmidt states

While in the bipartite setting all states admit a Schmidt decomposition, in the general multipartite setting this is not the case. We refer to those multipartite states that admit a Schmidt decomposition as Schmidt states. These, up to a local unitary, can be written in the form

$$|\Psi\rangle = \sum_{j=0}^{d-1} c_j\,|j\rangle^{\otimes N}\ ,$$

where $0 < c_j < 1$ for all i and $\sum_{j=0}^{d-1} c_j^2 = 1$.

Our proof that all multipartite entangled Schmidt states can be self-tested follows closely the ideas from [23], while leveraging as a building block our novel self-testing result for partially entangled GHZ states. Thus, we proceed by first proving a self-testing theorem for multipartite partially entangled qubit GHZ states.

Multipartite partially entangled GHZ qubit states Multipartite qubit Schmidt states, also known as partially entangled GHZ states, are of the form

$$|\mathrm{GHZ}_N(\theta)\rangle = \cos\theta\,|0\rangle^{\otimes N} + \sin\theta\,|1\rangle^{\otimes N}\ ,$$

where $\theta \in (0, \pi/4]$ and $|\mathrm{GHZ}_N(\pi/4)\rangle = |\mathrm{GHZ}_N\rangle$ is the standard N-qubit GHZ state. The form of this state is such that if any subset of $N-2$ parties performs a σ_X measurement, the collapsed state shared by the remaining two parties is $\cos\theta\,|00\rangle \pm \sin\theta\,|11\rangle$, depending on the parity of the measurement outcomes. As already mentioned, these states can be self-tested with the aid of the tilted CHSH inequality from Section 3.4, which is the main ingredient of our self-test of $|\mathrm{GHZ}_N(\theta)\rangle$. In the next Theorem, we describe constraints on an N-partite correlation that are obtained by post-selecting based on measurement outcomes for all but two parties', and imposing a maximal violation of the appropriate tilted CHSH inequality for the remaining two parties. From a multipartite strategy that satisfies these constraints, we construct operators, for each party, which behave like Pauli X and Pauli Z.

Theorem 19. *Let $|\psi\rangle$ be an N-partite state, and let $A_{0,i}, A_{1,i}$ be a pair of binary observables for the i-th party, for $i = 1, \ldots, N$. Suppose the following correlations are satisfied:*

$$\begin{aligned}
&\langle\psi|\, A_{0,i}^{(+)}\,|\psi\rangle = \langle\psi|\, A_{0,i}^{(+)} A_{0,j}^{(+)}\,|\psi\rangle = \cos^2\theta, \qquad \forall i,j \in \{1,\ldots,N-1\}\\
&\langle\psi|\prod_{i=1}^{N-2} A_{1,i}^{(a_i)}\,|\psi\rangle = \frac{1}{2^{N-2}}, \qquad \forall a \in \{+,-\}^{N-2}\\
&\langle\psi|\prod_{i=1}^{N-2} A_{1,i}^{(a_i)}(\alpha A_{0,N-1} + A_{0,N-1}A_{0,N} + A_{0,N-1}A_{1,N} + (-1)^{h(a)}A_{1,N-1}A_{0,N}\\
&\qquad\qquad - (-1)^{h(a)}A_{1,N-2}A_{1,N-1})\,|\psi\rangle = \frac{\sqrt{8+2\alpha^2}}{2^{N-2}}, \qquad \forall a \in \{+,-\}^{N-2}\ ,
\end{aligned}$$

where $h(a)$ denotes the parity of the number of "$-$" in a, and $\alpha = 2\cos 2\theta/\sqrt{1+\sin^2 2\theta}$. Let μ be such that $\tan\mu = \sin 2\theta$. Define $Z_i = A_{0,i}$ and $X_i = A_{1,i}$, for $i = 1, \ldots, N-1$. Then, let $Z'_N = (A_{0,N} + A_{1,N})/2\cos\mu$, and let Z^*_N be Z'_N with zero eigenvalues replaced by 1. Define $Z_N = Z^*_N|Z^*_N|^{-1}$. Define X_N similarly starting from $X'_N = (A_{0,N} - A_{1,N})/2\sin\mu$. Then,

$$Z_1\,|\psi\rangle = \cdots = Z_N\,|\psi\rangle\,, \tag{5.25}$$

$$X_1 \cdots X_D(I - Z_1)\,|\psi\rangle = \tan\theta(I + Z_1)\,|\psi\rangle\,. \tag{5.26}$$

Proof: We refer the reader to Appendix D.1 for the formal proof of this Theorem, while providing here an intuitive understanding of the correlations given above. The first equation (19) defines the existence of one measurement observable, whose marginal carries the information of angle θ. The straightforward consequence of it is Eq. (5.25), which is analogue to Eq. (41). On the other hand, eq. (19) involves a different measurement observable with zero marginal, while eq. (19) shows that when the first $N-2$ parties perform this zero marginal measurement the remaining two parties maximally violate the corresponding tilted CHSH inequality, i.e. the reduced state is self-tested to be the partially entangled pair of qubits. Eq. (5.26) is analogue to Eq. (41).

As a corollary, any correlation satisfying the constraints of Theorem 19 self-tests the state $|\mathrm{GHZ}_N(\theta)\rangle$.

Corollary 6. *Let $|\psi\rangle$ be an N-partite state, and let $A_{0,i}, A_{1,i}$ be a pair of binary observables for the ith party, for $i = 1,\ldots,N$. Suppose an N-partite correlation p^* satisfies the constraints of Theorem 19. Then, p^* self-tests $|\mathrm{GHZ}_N(\theta)\rangle$.*

Proof: This follows as a special case ($d = 2$) of Lemma 42 stated below, upon defining $P_i^{(k)} = [I + (-1)^k Z_i]/2$, for $k \in \{0,1\}$.

As one can expect, ideal measurements that achieve these constraints are: $A_{0,i} = \sigma_Z$, $A_{1,i} = \sigma_X$, for $i = 1,\ldots,N-1$, and $A_{0,N} = \cos\theta\sigma_Z + \sin\theta\sigma_X$, $A_{1,N} = \cos\theta\sigma_Z - \sin\theta\sigma_X$. We refer to the correlation induced by these ideal measurements as the *ideal correlation* for the multipartite entangled GHZ states (with these parameters).

All multipartite entangled qudit Schmidt states The generalisation of Theorem 19 to all multipartite qudit Schmidt states is then an adaptation of the proof in [23] for the bipartite case, with the difference that it uses as a building block the $|\mathrm{GHZ}_N(\theta)\rangle$ self-test that we just developed, instead of the tilted CHSH inequality.

We begin by stating a straightforward generalisation to the multipartite setting of the criterion from [102] which gives sufficient conditions for self-testing a Schmidt state. Then, our proof that all multipartite entangled qudit Schmidt states can be self-tested goes through showing the existence of operators satisfying the conditions of such criterion.

Lemma 42 (Generalisation of criterion from [102])**.** *Let $|\Psi\rangle$ be a state of the form (5.3.2.1). Suppose there exist sets of unitaries $\{X_l^{(k)}\}_{k=0}^{d-1}$, where the subscript $l \in \{1,\ldots,N\}$ indicates that the operator acts on the system of the l-th party, and sets of projections $\{P_l^{(k)}\}_{k=0}^{d-1}$, that are*

complete and orthogonal for $l = 1, \ldots, N-1$ and need not be such for $l = N$, and they satisfy:

$$P_1^{(k)} |\psi\rangle = \ldots = P_N^{(k)} |\psi\rangle ,$$
$$X_1^{(k)} \ldots X_N^{(k)} P_1^{(k)} |\psi\rangle = \frac{c_k}{c_0} P_1^{(0)} |\psi\rangle$$

for all $k = 1, \ldots, N$. Then, there exists a local isometry Φ such that $\Phi(|\psi\rangle) = |extra\rangle \otimes |\Psi\rangle$.

Proof. The proof of Lemma 42 is a straightforward generalisation of the proof of the criterion from [102], and is included in the Appendix for completeness.

We now describe the self-testing correlations for $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle^{\otimes n}$. Their structure is inspired by the self-testing correlations from [23] for the bipartite case, and they consist of three d-outcome measurements for all but the last party, which has four. We desribe them by first presenting the ideal measurements that achieve them, as we believe this aids understading. Subsequently, we extract their essential properties that guarantee self-testing. For a single-qubit observable A, denote by $[A]_m$ the observable defined with respect to the basis $\{|2m \mod d\rangle, |(2m+1) \mod d\rangle\}$. For example, $[\sigma_Z]_m = |2m\rangle\langle 2m| - |2m+1\rangle\langle 2m+1|$. Similarly, we denote by $[A]'_m$ the observable defined with respect to the basis $\{|(2m+1) \mod d\rangle, |(2m+2) \mod d\rangle\}$. We use the notation $\bigoplus A_i$ to denote the direct sum of observables A_i.

Let $\mathcal{X}_i$ denote the question set of the i-th party, and let $\mathcal{X}_i = \{0,1,2\}$ for $i = 1, \ldots, N-1$, and $\mathcal{X}_N = \{0,1,2,3\}$. Let $x_i \in \mathcal{X}_i$ denote a question to the i-th party. The answer sets are $\mathcal{A}_i = \{0,1,\ldots,d-1\}$, for $i = 1, \ldots, N$.

Definition 35 (Ideal measurements for multipartite entangled Schmidt states)**.** *The N parties make the following measurements on the joint state $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle^{\otimes n}$.*

For** $i = 1, \ldots, N-1$**:

- *For question $x_i = 0$, the i-th party measures in the computational basis $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ of its system,*
- *For $x_i = 1$ and $x_i = 2$: for d even, in the eigenbases of observables $\bigoplus_{m=0}^{\frac{d}{2}-1} [\sigma_X]_m$ and $\bigoplus_{m=0}^{\frac{d}{2}-1} [\sigma_X]'_m$ respectively, with the natural assignments of d measurement outcomes; for d odd, in the eigenbases of observables $\bigoplus_{m=0}^{\frac{d-1}{2}-1} [\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ and $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1} [\sigma_X]'_m$ respectively.*

For** $i = N$**:

- *For $x_N = 0$ and $x_N = 1$, the party N measures in the eigenbases of $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu_m)\sigma_Z + \sin(\mu_m)\sigma_X]_m$ and $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu_m)\sigma_Z - \sin(\mu_m)\sigma_X]_m$ respectively, with the natural assignments of d measurement outcomes, where $\mu_m = \arctan[\sin(2\theta_m)]$ and $\theta_m = \arctan(c_{2m+1}/c_{2m})$; for d odd, he measures in the eigenbases of $\bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu_m)\sigma_Z + \sin(\mu_m)\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ and $\bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu_m)\sigma_Z - \sin(\mu_m)\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ respectively.*

- *For $x_N = 2$ and $x_N = 3$: for d even, the N-th party measures in the eigenbases of $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu'_m)\sigma_Z + \sin(\mu'_m)\sigma_X]'_m$ and $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu'_m)\sigma_Z - \sin(\mu'_m)\sigma_X]'_m$ respectively, where $\mu'_m = \arctan[\sin(2\theta'_m)]$ and $\theta'_m = \arctan(c_{2m+2}/c_{2m+1})$; for d odd, in the eigenbases of $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu'_m)\sigma_Z + \sin(\mu'_m)\sigma_X]'_m$ and $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu'_m)\sigma_Z - \sin(\mu'_m)\sigma_X]'_m$, respectively.*

We refer to the correlation specified by the ideal measurements above as the ideal correlation for multipartite entangled Schmidt states.

Next, we will highlight a set of properties of the ideal correlation that are enough to characterize it, in the sense that any quantum correlation that satisfies these properties has to be the ideal one. This also aids understanding of the self-testing proof (Proof of Theorem 20). In what follows, we will employ the language of correlation tables, which gives a convenient way to describe correlations. In general, let $\mathcal{X}_i$ be the question sets and $\mathcal{A}_i$ the answer sets. A correlation specifies, for each possible question $x \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_N$, a table T_x with entries $T_x(a) = p(a|x)$ for $a \in \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$. For example, we denote the correlation tables for the ideal correlations for multipartite entangled GHZ states from Theorem 19 as $T_x^{\mathrm{ghz}_N(\theta_m)}$, where $x \in \{0,1\}^N$ denotes the question.

Definition 36 (Self-testing properties of the ideal correlations for multipartite entangled Schmidt states)**.** *Recall that $\mathcal{X}_i = \{0,1,2\}$ for $i = 1,\ldots,N-1$, and $\mathcal{X}_N = \{0,1,2,3\}$. $\mathcal{A}_i = \{0,1,\ldots,d-1\}$, for $i = 1,\ldots,N$.*

The self-testing properties of the ideal correlations are:

- *For questions $x \in \{0,1\}^N$, we require T_x to be block-diagonal with $2^{\times N}$ blocks $C_{x,m} := (c_{2m}^2 + c_{2m+1}^2)\cdot T_x^{ghz_N(\theta_m)}$ corresponding to outcomes in $\{2m, 2m+1\}^N$, where the multiplication by the weight is intended entry-wise, and $\theta_m := \arctan\left(c_{2m+1}/c_{2m}\right)$.*

- *For questions with $x_i \in \{0,2\}$, for $i = 1,\ldots,N-1$ and $x_N \in \{2,3\}$ we require T_x to be block-diagonal with the $2^{\times N}$ blocks "shifted down" by one measurement outcome. These should be $D_{x,m} := (c_{2m+1}^2 + c_{2m+2}^2)\cdot T^{ghz_N(\theta'_m)}_{f(x_1),\ldots,f(x_{N-1}),g(x_N)}$ corresponding to measurement*

outcomes in $\{2m+1, 2m+2\}^N$, *where* $\theta'_m := \arctan\left(c_{2m+2}/c_{2m+1}\right)$ *and* $f(0) = 0$, $f(2) = 1$, $g(2) = 0$, $g(3) = 1$.

We are now ready to state the main theorem of this section.

Theorem 20. *Let* $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle^{\otimes N}$, *where* $0 < c_j < 1$ *for all* i *and* $\sum_{j=0}^{d-1} c_j^2 = 1$. *Suppose* N *parties exhibit the ideal correlations for multipartite entangled Schmidt states from Definition 35 by making local measurements on a joint state* $|\psi\rangle$. *Then there exists a local isometry* Φ *such that* $\Phi(|\psi\rangle) = |extra\rangle \otimes |\Psi\rangle$.

As we mentioned, the proof of Theorem 20 follows closely the method of [23], and uses as a building block our self-testing of the n-partite partially entangled GHZ state. For the details, we refer the reader to Appendix D.3.

5.3.3 Discussion

We investigated a simple, but potentially general, approach to self-testing multipartite states, inspired by [101], which relies on the well understood method of self-testing bipartite qubit states based on the maximal violation of the tilted CHSH Bell inequality. This approach allows one to self-test, with few measurements per party, all partially entangled GHZ qubit states. In our work, we also generalize self-testing of partially entangled GHZ qubit states to the qudit case, using techniques from [23]. We obtain the first self-testing result for a class of multipartite qudit states, by showing that all multipartite qudit states that admit a Schmidt decomposition can be self-tested. Importantly, our self-tests have a low complexity in terms of resources as they require up to four measurement choices per party, and the total number of expectation values of the observables that one needs to determine scales linearly with the number of parties. Although this result is not included in this thesis, our approach also allows to self-test all permutationally invariant Dicke states, and it allows to recover self-testing of all graph states (a result which was previously known through stabilizer state methods [60]).

As a direction for future work, we are particularly interested in extending this approach to self-test any generic multipartite entangled state of qubits (which is local-unitary equivalent to its complex conjugate in any basis). The main challenge here is to provide a general recipe to construct a single isometry that self-tests the global state from the different ones derived from various subtests (i.e. from projecting various subsets of parties and looking at the correlations of the remaining ones). This appears to be challenging for states that do not have any particular symmetry.

Chapter 6

FOUNDATIONAL QUESTIONS, AND THE QUEST FOR INFINITE ENTANGLEMENT

In this chapter, we finally explore some of the connections of self-testing with foundational questions in the theory of entanglement. One of the most basic questions one can ask about a correlation is "in which models of physics can the correlation be realized?". Some correlations can be realized in classical physics if one allows the provers to share randomness ahead of time. However, at this point in the thesis, we understand very well that some correlations require quantum resources to realize [9]. In fact, different models of quantum mechanics admit different sets of correlations. Characterizing the relationship between these sets is a long-standing problem.

We say that a correlation is in the set of *quantum correlations* $\mathcal{C}_q$ if there is a finite-dimensional state $|\psi\rangle$ and finite-dimensional projective measurements $\left\{\Pi^a_{A_x}\right\}, \left\{\Pi^b_{B_y}\right\}$ so that

$$p(a,b|x,y) = \langle\psi| \Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle \ , \tag{6.1}$$

where $p(a,b|x,y)$ is the probability that Alice answers a and Bob answers b, given that Alice was asked question x and Bob was asked question y. The correlations in $\mathcal{C}_q$, are often referred to as *finite-dimensional* quantum correlations

We say that a correlation is in the set of *quantum spatial correlations* $\mathcal{C}_{qs}$ if Equation (6.1) holds with a state and measurements that are possibly infinite-dimensional, on separable Hilbert spaces. These are often referred to as *infinite-dimensional quantum correlations*. Notice that $\mathcal{C}_q \subseteq \mathcal{C}_{qs}$.

We say that a correlation is in the set of *quantum-approximate correlations* $\mathcal{C}_{qa}$ if it is arbitrarily well-approximated by correlations in $\mathcal{C}_q$. In other words, $\mathcal{C}_{qa}$ is the closure of $\mathcal{C}_q$. From [84], we know that $\mathcal{C}_{qs} \subseteq \mathcal{C}_{qa}$, hence $\mathcal{C}_{qa}$ is also the closure of $\mathcal{C}_{qs}$.

On the other hand, taking a step back, one can even drop the assumption of a tensor product decomposition, and only require that measurements on spatially separated quantum systems commute with each other. For instance, the latter approach is typical in algebraic quantum field theory [43]. The resulting set of correlations is known as the set of *quantum commuting* correlations, or $\mathcal{C}_{qc}$. A sequence of two breakthrough works by Slofstra [89, 90] has shed light on the relationship between these variants and the tensor product model, culminating in a proof that the set of quantum correlations is not closed. Following Slofstra's work, the known hierarchy between these variants is:

$$\mathcal{C}_q \subseteq \mathcal{C}_{qs} \subsetneq \mathcal{C}_{qa} \subseteq \mathcal{C}_{qc} \, . \tag{6.2}$$

It is known that the last inclusion ($\mathcal{C}_{qa} \subseteq \mathcal{C}_{qc}$) is an equality if and only if Connes' embedding conjecture is true. The latter is a long-standing open question in operator algebras [73].

This "four correlation sets" picture, along with the explicit study of $\mathcal{C}_{qs}$, was introduced by Paulsen and coauthors [78, 77, 34].

Organization The main theorem for this chapter, and one of the main results of this thesis is that the first inclusion in Equation (6.2) is strict: $\mathcal{C}_q \neq \mathcal{C}_{qs}$. In particular, we give an explicit correlation which can be attained in infinite dimensions, and we show that it cannot be attained in finite dimensions. We cover this in Section 6.1. In Section 6.2, we exploit our novel generalization of CHSH from Section 5.2, as well as the tilted CHSH inequality, to construct a strikingly simple non-local game with the following property: any ϵ-close to optimal strategy requires an entangled state of dimension at least $2^{\Omega(1/poly(\epsilon))}$. This matches the strongest known tradeoff between precision and dimension. As a corollary, the existence of our game yields a new proof of the non-closure of the set of quantum correlations, namely $\mathcal{C}_{qs} \neq \mathcal{C}_{qa}$. The proof is arguably elementary, and is based on self-testing techniques and a phenomenon known as embezzlement, discovered in [30], and which we will review.

6.1 An inherently infinite-dimensional quantum correlation

6.1.1 Introduction

The question of whether $\mathcal{C}_q = \mathcal{C}_{qs}$, i.e. whether the set of finite and infinite-dimensional quantum correlations are equal or not, was first posed by Tsirelson in 1993 [95] (amongst other open questions), and has been unresolved since then. A positive answer to this question would establish that infinite-dimensional entanglement is a strictly more expressive resource than finite-dimensional entanglement. This would imply, for example, that two entangled infinite-level systems (one can think of two entangled harmonic oscillators) can exhibit correlations that cannot be reproduced exactly by two entangled finite-level systems.

Interest in this question was further fueled by the discovery and the study of the I_{3322} Bell inequality in [38]. This corresponds to a scenario in which the two parties get one of three questions and they respond with one of two possible answers. It exhibits the following peculiar behaviour: no fixed finite-dimensional quantum strategy appears to attain the maximal quantum violation of the inequality. In [74], Pál and Vértesi give extensive numerical evidence suggesting that finite-dimensional states are not enough to attain maximal violation of the inequality, and they conjecture that infinite-dimensional states suffice. However, an analytical proof has remained elusive.

Our result We settle the long-standing open question about the relationship between $\mathcal{C}_q$ and $\mathcal{C}_{qs}$, asserting that $\mathcal{C}_q \neq \mathcal{C}_{qs}$. In particular, we give an explicit correlation on five questions per party and three answers per party, which can be attained exactly in infinite dimensions, and we show that it cannot be attained in finite dimensions. In other words, we provide an example of an *inherently* infinite-dimensional quantum correlation. This exhibits precisely the behaviour conjectured by Pál and Vértesi [74], on slightly larger question and answer sets.

More formally, letting $\mathcal{C}_q^{m,n,r,s}$ ($\mathcal{C}_{qs}^{m,n,r,s}$) be the set of finite-dimensional (resp. infinite-dimensional) quantum correlations on question sets of sizes m and n and answer sets of sizes r and s, we show:

Theorem 21. $\mathcal{C}_q^{4,5,3,3} \neq \mathcal{C}_{qs}^{4,5,3,3}$.

Notice that we define $\mathcal{C}_q = \bigcup_{m,n,r,s<\infty} \mathcal{C}_q^{m,n,r,s}$ and similarly for $\mathcal{C}_{qs}$, so the above implies $\mathcal{C}_q \neq \mathcal{C}_{qs}$.

Related work The problem we settle fits into a well-established line of research: the quest to understand and to find correlations that require infinite entanglement to attain. In [56], Mančinska and Vidick give the first example of a game whose optimal winning probability can be approximated arbitrarily well, but not achieved perfectly, with finite-dimensional states. However, the set of possible answers for the parties in this game is countably infinite. The first example of a game of finite size exhibiting the same behaviour was provided by Slofstra [90], while a series of subsequent

works [89, 33, 50, 91, 87, 68, 20] refined this result in various ways (for example reducing the size of the game or quantifying the tradeoff between between winning probability in the game and dimension required).

However, the sequences of ideal strategies for all of these games do not have a limit, since they are produced by maximally entangled states of higher and higher dimension. Hence, the limiting correlations separate $\mathcal{C}_{qs}$ from $\mathcal{C}_{qa}$ but do not shed any light on the relationship between $\mathcal{C}_q$ and $\mathcal{C}_{qs}$. Ours is the first example of a correlation that is inherently infinite dimensional: it cannot be attained in finite dimensions, but it can be attained exactly in infinite dimensions (in the tensor product model).

The caveat on experimentally testing the existence of infinite-dimensional systems At first sight it appears that our correlation provides a test that can tell apart an infinite-dimensional system from a finite-dimensional one, and hence, in principle, a test that can assert whether nature allows existence of systems with infinitely many degrees of freedom. However, this is not the case. In fact, although our correlation can only be exactly attained by two entangled infinite-dimensional systems, for example two entangled systems with infinite energy levels, it can be approximated arbitrarily well by systems of high enough, but finite, dimension, or in other words, by projecting onto subspaces of bounded energy. Thus, no experiment (which can only estimate statistics to a finite precision) can tell the two cases apart. This is not a shortcoming of our separating correlation, but rather a fundamental limitation that stems from the fact that the sets $\mathcal{C}_q$ and $\mathcal{C}_{qs}$ possess the same closure.

It is striking that we observe such a fundamental theoretical difference between finite and infinite-dimensional models of entanglement, yet we are inherently limited in our ability to distinguish the two models by the finiteness of the data we can gather.

6.1.2 A brief overview of the proof of separation

We start with a very concise overview of the structure of the proof of our main result. To explain the argument, we start by giving an idealized version that runs against a barrier, and then talk about how to avoid the barrier.

We will start by introducing an ideal correlation p^* of a particular form. Suppose we knew that any quantum strategy achieving p^* must satisfy the following two conditions: First, there is a local isometry $\Phi = \Phi_A \otimes \Phi_B$ and an auxiliary state $|aux\rangle$ such that

$$\Phi(|\psi\rangle) = \frac{1}{\sqrt{1+\alpha^2}}(|00\rangle + \alpha\,|11\rangle) \otimes |aux\rangle\,. \tag{6.3}$$

Next, there is another local isometry Φ' and an auxiliary state $|aux'\rangle$ such that

$$\Phi'(|\psi\rangle) = |\phi\rangle \oplus \frac{1}{\sqrt{1+\alpha^2}}(|00\rangle + \alpha\,|11\rangle) \otimes |aux'\rangle\,, \tag{6.4}$$

where $\oplus$ denotes a direct sum and the state $|\phi\rangle$ is separable, i.e. has Schmidt rank 1. Then suppose towards a contradiction that $|\psi\rangle$ were finite-dimensional. Since Schmidt coefficients are preserved under local isometries, from the first condition we see that the Schmidt rank of the state is even, while from the second condition we see that the Schmidt rank of the state is odd; contradiction.

In the above, the "magic" happens when we assume that $|\phi\rangle$ is separable. In general, any correlation that is attained using a separable $|\phi\rangle$ could also be attained by tensoring with extra entanglement and not making use of it in the measurements, so we will not be able to assume that $|\phi\rangle$ is separable. A different way of arguing about the set of Schmidt coefficients of $|\psi\rangle$ is required. Our main argument will still decompose $|\psi\rangle$ into two ways as in equations (6.3) and (6.4). In place of the odd / even constraints, we will show that these decompositions partition the Schmidt coefficients into two different ways so that the set of nonzero Schmidt coefficients of $|\psi\rangle$ is in bijection with a proper subset of itself.

Organization Section 6.1.3 covers some preliminary notions. Section 6.1.4 formalizes the notion of a direct sum of correlations and proves that a certain block structure in a correlation implies a similar direct sum decomposition of the state and measurements achieving the correlation. In Section 6.1.5, we describe the separating correlation by specifying the infinite dimensional state and measurements that attain it exactly. In Section 6.1.6.1, we apply self-testing techniques to establish properties of any state and measurements achieving the separating correlation; these properties will be similar to Equations (6.3) and (6.4). Finally in Section 6.1.6.2, we will use these properties of the state to show that it has infinitely many nonzero Schmidt coefficients.

6.1.3 Preliminaries

For an operator $T \in \mathcal{L}(\mathcal{H})$ and a subspace $\mathcal{H}' \subseteq \mathcal{H}$ invariant under T, we denote by $T|_{\mathcal{H}'} \in \mathcal{L}(\mathcal{H}')$ the restriction of T to $\mathcal{H}'$. Let $\mathbb{C}^{\mathbb{N}}$ denote the Hilbert space of square-summable sequences, sometimes called $\ell^2(\mathbb{C})$. We endow it with a standard basis $\{|i\rangle : i \in \mathbb{N}\}$. Formally, $\mathbb{C}^{\mathbb{N}} = \left\{\sum_i a_i\,|i\rangle : \sum_i \left|a_i^2\right| < \infty\right\}$.

We denote by $\mathcal{C}_q^{m,n,r,s}$ and $\mathcal{C}_{qs}^{m,n,r,s}$ respectively the sets of finite and infinite-dimensional quantum correlations on question sets of sizes m, n and answer sets of sizes r, s.

6.1.3.1 Tilted CHSH

We have already introduced the tilted CHSH inequality in Section 3.4. Here, we recall for convenience its essential properties, as this is a building block for the separating correlation in this section. For entangled $|\psi\rangle$, we have:

$$\langle \psi \,|\, \beta A_0 + A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \,|\, \psi \rangle \leq \sqrt{8 + 2\beta^2}. \tag{6.5}$$

The maximum in the tilted CHSH inequality is attained by the following strategy:

Definition 37 (Ideal strategy for tilted CHSH)**.** *Given parameter β, let* $\sin 2\theta = \sqrt{\frac{4-\beta^2}{4+\beta^2}}$, $\mu = \arctan \sin 2\theta$, *and* $\alpha = \tan\theta$. *Define the* α-tilted Pauli operators *as*

$$\sigma_\alpha^z := \cos\mu\sigma^z + \sin\mu\sigma^x, \text{ and } \sigma_\alpha^x := \cos\mu\sigma^z - \sin\mu\sigma^x.$$

The ideal strategy for tilted CHSH with parameter β (i.e. achieving maximal violation of (6.5)*) consists of the joint state $|\Psi\rangle = \cos\theta(|00\rangle + \alpha\,|11\rangle)$ and observables A_0, A_1 and B_0, B_1 with $A_0 = \sigma^z$, $A_1 = \sigma^x$, $B_0 = \sigma_\alpha^z$ and $B_1 = \sigma_\alpha^x$. For each observable, we associate the projection onto the $+1$-eigenspace with answer 0 and the projection onto the -1-eigenspace with answer 1.*

Since in the present section we are primarily concerned with the ratio of the coefficients of the ideal state, we refer to the correlation defined by the ideal strategy of Definition 37 as the *ideal tilted CHSH correlation for ratio α*. In the remainder of the paper, we use the correlation along with the ideal strategy, but we will forget the Bell inequality (6.5) that motivates them. In particular, we will use the following lemma.

Lemma 43 ([7])**.** *The tilted CHSH correlation for ratio α self-tests the strategy of Definition 37.*

6.1.3.2 Correlation tables

Recall the definition of correlation tables from Section 2.2. As mentioned earlier, we will make use of the ideal tilted CHSH correlation as a building block for our separating correlation. For $x, y \in \{0,1\}$ and $\alpha \in (0,1)$, we denote by $\mathrm{CHSH}^\alpha_{x,y}$ the correlation table on question x, y for the ideal tilted CHSH correlation for ratio α.

6.1.4 Direct sums of correlations

In this section, we introduce the notion of a direct sum of correlations. We will later use this to build our desired correlation out of tilted CHSH building blocks. Lemma 39 will allow us to characterize the strategies for the desired correlation from self-testing results about its direct summands. In particular, these strategies also decompose, in a sense made precise below, as a direct sum of

strategies corresponding to the direct summands. The proof is somewhat technical, and the ideas in the proof are not necessary to understand the rest of the paper. Some of the ideas in this proof have already appeared in Sections 5.1 and 5.2, where they were used to establish properties of quantum correlations constructed block-by-block [23], [21]. We package these arguments into a lemma since it may be of independent interest. First, we define formally a direct sum of correlations.

Definition 38 (Direct sum of correlations)**.** *Let p be a correlation on $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$. Suppose for some positive integer l, for $i \in [l]$, there exist partitions $\mathcal{A} = \bigsqcup_{i=1}^{l} \mathcal{A}_i$, $\mathcal{B} = \bigsqcup_{i=1}^{l} \mathcal{B}_i$, real numbers $\omega_i \geq 0$ with $\sum_{i=1}^{l} \omega_i = 1$, and correlations p_i on $\mathcal{X}, \mathcal{Y}, \mathcal{A}_i, \mathcal{B}_i$ such that for all $i, j \in [l]$, $a \in \mathcal{A}_i, b \in \mathcal{B}_j, x \in \mathcal{X}, y \in \mathcal{Y}$,*

$$p(a, b|x, y) = \delta_{ij} \omega_i p_i(a, b|x, y). \tag{6.6}$$

Then we say that p is a direct sum of the p_i, and we write $p = \oplus_{i=1}^{l} \omega_i p_i$. We sometimes refer to the p_i as blocks *of p and the ω_i as* weights *of the blocks. We give a visual interpretation of condition* (6.6) *in Table 6.1.*

a \ b	$\mathcal{B}_1$	$\cdots$	$\mathcal{B}_l$
$\mathcal{A}_1$	$\omega_1 \cdot T_{xy}^{(1)}$	0	0
$\vdots$	0	$\ddots$	0
$\mathcal{A}_l$	0	0	$\omega_l \cdot T_{xy}^{(l)}$

Table 6.1: The correlation table for $p = \oplus_i \omega_i p_i$ on questions x, y. $T_{xy}^{(i)}$ is the correlation table for correlation p_i on questions x, y.

Lemma 44. *Let $p \in \mathcal{C}_{qs}^{m,n,d,d}$ be a correlation on $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$, induced by a strategy $(|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{\Pi_{A_x}^a\}_a, \{\Pi_{B_y}^b\}_b)$. Suppose for some positive integer l, there exist partitions $\mathcal{A} = \bigsqcup_{i=1}^{l} \mathcal{A}_i$, $\mathcal{B} = \bigsqcup_{i=1}^{l} \mathcal{B}_i$, with $|\mathcal{A}_i| = |\mathcal{B}_i| = d_i$, and correlations $p_i \in \mathcal{C}_{qs}^{m,n,d_i,d_i}$ on $\mathcal{X}, \mathcal{Y}, \mathcal{A}_i, \mathcal{B}_i$ such that $p = \bigoplus_{i=1}^{l} \omega_i p_i$. Then there exist direct sum decompositions $\mathcal{H}_A = \mathcal{H}_A^{null} \oplus \bigoplus_i \mathcal{H}_A^i, \mathcal{H}_B = \mathcal{H}_B^{null} \oplus \bigoplus_i \mathcal{H}_B^i$ and strategies*

$$\left(\frac{|\psi_i\rangle}{\||\psi_i\rangle\|} \in \mathcal{H}_A^i \otimes \mathcal{H}_B^i, \{\Pi_{A_x}^a|_{\mathcal{H}_A^i}\}_{a \in \mathcal{A}_i}, \{\Pi_{B_y}^b|_{\mathcal{H}_B^i}\}_{b \in \mathcal{B}_i} \right) \tag{6.7}$$

such that:

(i) Strategy (6.7) *is well-defined, i.e. the restricted operators $\Pi_{\mathcal{A}_x}^a|_{\mathcal{H}_A^i}$ and $\Pi_{\mathcal{A}_y}^b|_{\mathcal{H}_B^i}$ are projections.*

(ii) $\| |\psi_i\rangle \|^2 = \omega_i$.

(iii) p_i *is induced by strategy* (6.7).

(iv) For all $x \in \mathcal{X}, y \in \mathcal{Y}, a \in \mathcal{A}_i, b \in \mathcal{B}_i$*:*

$$\Pi^a_{A_x}|_{\mathcal{H}^i_A} |\psi_i\rangle = \Pi^a_{A_x} |\psi\rangle\,, \quad \Pi^B_{B_y}|_{\mathcal{H}^i_B} |\psi_i\rangle = \Pi^b_{B_y} |\psi\rangle$$

Proof. For the remainder of the proof, when an operator acts only on one tensor factor we omit writing the identity on the other factors.

Our first goal is to construct the subspaces $\mathcal{H}^i_A, \mathcal{H}^i_B$. We first study the action of the projectors corresponding to answers in $\mathcal{A}_i$ and $\mathcal{B}_i$ on the state $|\psi\rangle$. We will use these properties to define the states $|\psi_i\rangle$. Then from these, we will construct $\mathcal{H}^i_A$ and $\mathcal{H}^i_B$.

For $x \in \mathcal{X}, y \in \mathcal{Y}$, define $\Pi^{\mathcal{A}_i}_{A_x} := \sum_{a\in\mathcal{A}_i} \Pi^a_{A_x}$ and $\Pi^{\mathcal{B}_i}_{B_y} := \sum_{b\in\mathcal{B}_i} \Pi^b_{B_y}$. We will show that $\Pi^{\mathcal{A}_i}_{A_x} |\psi\rangle = \Pi^{\mathcal{B}_i}_{B_y} |\psi\rangle$ for all i, x, y. For any $i \in [l], x \in \mathcal{X}, y \in \mathcal{Y}$,

$$\begin{aligned}
\Pi^{\mathcal{A}_i}_{A_x} |\psi\rangle &= \left(\sum_{a\in\mathcal{A}_i} \Pi^a_{A_x}\right) \otimes I\, |\psi\rangle \\
&= \left(\sum_{a\in\mathcal{A}_i} \Pi^a_{A_x}\right) \otimes \left(\sum_{b\in\mathcal{B}} \Pi^b_{B_y}\right) |\psi\rangle \qquad (6.8)\\
&= \left(\sum_{a\in\mathcal{A}_i} \Pi^a_{A_x}\right) \otimes \left(\sum_{b\in\mathcal{B}_i} \Pi^b_{B_y}\right) |\psi\rangle \\
&= \Pi^{\mathcal{A}_i}_{A_x} \otimes \Pi^{\mathcal{B}_i}_{B_y} |\psi\rangle\,. \qquad (6.9)
\end{aligned}$$

The second equality follows from the fact that $\left\{\Pi^b_{B_y}\right\}$ forms a complete measurement. The third equality comes from the block structure of the correlation. More specifically, suppose that $a \in \mathcal{A}_i$ but $b \notin \mathcal{B}_i$. Then the block structure demands that $p(a, b|x, y) = 0$ for all x, y. So we conclude that $\left\|\Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle\right\|^2 = p(a, b|x, y) = 0$. This forces the appropriate terms of the sum in Equation (6.8) to vanish. The same argument with the roles of $\mathcal{A}$ and $\mathcal{B}$ reversed gives

$$\Pi^{\mathcal{B}_i}_{B_y} |\psi\rangle = \Pi^{\mathcal{A}_i}_{A_x} \otimes \Pi^{\mathcal{B}_i}_{B_y} |\psi\rangle\,.$$

Combined with Equation (6.9), this implies that, for any i, x, y,

$$\Pi^{\mathcal{A}_i}_{A_x} |\psi\rangle = \Pi^{\mathcal{B}_i}_{B_y} |\psi\rangle\ . \qquad (6.10)$$

In particular, the action of $\Pi^{\mathcal{A}_i}_{A_x}$ on $|\psi\rangle$ is the same for all x, and similarly for the $\mathcal{B}$ operators. This lets us define

$$|\psi_i\rangle := \Pi^{\mathcal{A}_i}_{A_x} |\psi\rangle\,,$$

where the choice of x does not matter.

Now we compute the norm of $|\psi_i\rangle$. The block structure $p = \oplus_i \omega_i p_i$ of the correlation gives us that for any fixed x and y,

$$\begin{aligned}\omega_i &= \sum_{a\in\mathcal{A}_i, b\in\mathcal{B}_i} p(a,b|x,y) \\ &= \sum_{a\in\mathcal{A}_i, b\in\mathcal{B}_i} \left\langle \psi \right| \Pi^a_{A_x} \otimes \Pi^b_{B_y} \left| \psi \right\rangle \\ &= \left\langle \psi \right| \Pi^{\mathcal{A}_i}_{A_x} \otimes \Pi^{\mathcal{B}_i}_{B_y} \left| \psi \right\rangle \\ &= \| |\psi_i\rangle \|^2 ,\end{aligned}$$

where the last line follows from Equation (6.10). This establishes condition (ii). Now let $\rho^i_A = \mathrm{Tr}_B |\psi_i\rangle\langle\psi_i| = \sum_j \lambda_j |j\rangle\langle j|$, where λ_j are the eigenvalues and $|j\rangle$ the eigenvectors of ρ^i_A. These are guaranteed to exist even if $|\psi_i\rangle$ is infinite-dimensional, because the existence of a Schmidt decomposition for any bipartite state holds also in infinite-dimensional Hilbert spaces. Notice that

$$\sum_j \lambda_j = \mathrm{Tr}\, \rho^i_A = \| |\psi_i\rangle \|^2 = \omega_i .$$

We wish to compute the action of $\Pi^{\mathcal{A}_i}_{A_x}$ on the eigenstates of ρ^i_A. We calculate

$$\begin{aligned}\omega_i &= \left\langle \psi \right| \Pi^{\mathcal{A}_i}_{A_x} \otimes I \left| \psi \right\rangle \\ &= \mathrm{Tr}\, \Pi^{\mathcal{A}_i}_{A_x} \rho^i_A \\ &= \sum_j \lambda_j \,\mathrm{Tr}\, \Pi^{\mathcal{A}_i}_{A_x} |j\rangle\langle j| \\ &= \sum_j \lambda_j \left\| \Pi^{\mathcal{A}_i}_{A_x} |j\rangle \right\|^2 .\end{aligned}$$

Since $\omega_i = \sum_j \lambda_j$, we must have $\left\| \Pi^{\mathcal{A}_i}_{A_x} |j\rangle \right\|^2 = 1$ for each j. In other words, $\Pi^{\mathcal{A}_i}_{A_x} |j\rangle = |j\rangle$. This motivates us to define the space $\mathcal{H}^i_A$ as the span of the nontrivial eigenvectors of ρ^i_A. Define also P_i as the projection onto subspace $\mathcal{H}^i_A$.

It follows from the definition of the $|\psi_i\rangle$ and the $\mathcal{H}^i_A$ that

$$P_i |\psi_j\rangle = \delta_{ij} |\psi_i\rangle \ . \tag{6.11}$$

Furthermore, notice that $\Pi^{\mathcal{A}_i}_{A_x} P_i = P_i$. Thus the $\mathcal{H}^i_A$ are suitable spaces for the new strategies to be defined on. In particular, the restricted operators $\Pi^a_{A_x}|_{\mathcal{H}^i_A}$ are projectors. To see this, notice that they are orthogonal for distinct a and that they sum to identity.

Let $\mathcal{H}_A^{\text{null}}$ be the orthogonal complement of $\bigoplus_i \mathcal{H}_A^i$ in $\mathcal{H}_A$. Define $\mathcal{H}_B^i$ and $\mathcal{H}_B^{\text{null}}$ analogously. Clearly, $\bigoplus_i \mathcal{H}_A^i$ and $\bigoplus_i \mathcal{H}_B^i$ are topologically closed. This implies that $\mathcal{H}_A = \mathcal{H}_A^{\text{null}} \oplus \bigoplus_i \mathcal{H}_A^i$ and $\mathcal{H}_B = \mathcal{H}_B^{\text{null}} \oplus \bigoplus_i \mathcal{H}_B^i$.

Thus, we have established condition (i) of the lemma.

It follows straightforwardly from the Definition of $|\psi_i\rangle$ and (6.11) that for $a \in \mathcal{A}_i$, $\Pi^a_{A_x}|_{\mathcal{H}_A^i} |\psi_i\rangle = \Pi^a_{A_x} |\psi\rangle$, and similarly for $\mathcal{B}$. This establishes condition (iv). Finally, we show condition (iii), that the strategies in each block induce the appropriate correlations. We fix arbitrary $a \in \mathcal{A}_i, b \in \mathcal{B}_i, x \in \mathcal{X}, y \in \mathcal{Y}$, and calculate

$$\begin{aligned}\frac{1}{\||\psi_i\rangle\|^2} \left\langle \psi_i \middle| \Pi^a_{A_x}|_{\mathcal{H}_A^i} \otimes \Pi^b_{B_y}|_{\mathcal{H}_B^i} \middle| \psi_i \right\rangle &= \frac{1}{\omega_i} \left\langle \psi \middle| \Pi^a_{A_x} \otimes \Pi^b_{B_y} \middle| \psi \right\rangle \\ &= \frac{1}{\omega_i} p(a,b|x,y) \\ &= p_i(a,b|x,y).\end{aligned}$$

In the above, the first quantity is the correlation induced by the strategy defined in Equation (6.7), and the last quantity is the desired correlation p_i. Thus, we have shown condition (iii).

□

6.1.5 The separating correlation

In this section, we describe the correlation p^* that separates $\mathcal{C}_q$ and $\mathcal{C}_{qs}$. The correlation is on question sets $\mathcal{X} = \{0,1,2,3\}$ and $\mathcal{Y} = \{0,1,2,3,4\}$ and answer sets $\mathcal{A} = \mathcal{B} = \{0,1,2\}$. Hence, the smallest classes we separate are $\mathcal{C}_q^{4,5,3,3}$ and $\mathcal{C}_{qs}^{4,5,3,3}$. We define p^* by describing the ideal infinite-dimensional strategy that induces it. In the following section, we will prove that no finite-dimensional strategy induces p^*.

Recall the definition of $\mathbb{C}^{\mathbb{N}}$ from Section 6.1.3. For each $m \geq 0$, we define two isometries $V_m^{\text{even}}, V_m^{\text{odd}} : \mathbb{C}^2 \to \mathbb{C}^{\mathbb{N}}$ as follows:

$$V_m^{\text{even}} |0\rangle = |2m\rangle \,, V_m^{\text{even}} |1\rangle = |2m+1\rangle \,, \text{and } V_m^{\text{odd}} |0\rangle = |2m+1\rangle \,, V_m^{\text{odd}} |1\rangle = |2m+2\rangle \,.$$

We use these isometries to define observables on $\mathbb{C}^{\mathbb{N}}$. By abuse of notation, for an isometry $V : \mathbb{C}^2 \to C^{\mathbb{N}}$ and an operator O on $\mathbb{C}^2$, we write $V(O)$ to refer to the pushforward $VOV^\dagger$ of O along V. For example, $V_m^{\text{even}}(\sigma^z) = |2m\rangle\langle 2m| - |2m+1\rangle\langle 2m+1|$. For O an operator with $+1, 0, -1$ eigenvalues, we write O^+ for the projection onto the $+1$ eigenspace and O^- for the projection onto the -1 eigenspace. One can check that with this notation $O = O^+ - O^-$. We use the notation $\bigoplus A_i$ to denote the direct sum of observables A_i. We will make use of the α-tilted Paulis $\sigma_\alpha^z, \sigma_\alpha^x$ from Definition 37. The following is the ideal strategy in detail.

Definition 39 (Ideal state and measurements for $p^* \in \mathcal{C}_{qs}^{4,5,3,3}$)**.** *Fix $\alpha \in (0,1)$. The correlation $p^* \in \mathcal{C}_{qs}^{4,5,3,3}$ is specified by the quantum strategy $(|\Psi\rangle \in \mathbb{C}^{\mathbb{N}} \otimes \mathbb{C}^{\mathbb{N}}, \{\Pi_{A_x}^a\}_a, \{\Pi_{B_y}^b\}_b)$, where $|\Psi\rangle = \sqrt{1-\alpha^2}\sum_{i=0}^{\infty} \alpha^i |ii\rangle$, and the ideal measurements are described in Tables 6.2 and 6.3.*

x \ a	0	1	2
0	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma^z)]^+$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma^z)]^-$	0
1	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma^x)]^+$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma^x)]^-$	0
2	$[\bigoplus_{m=0}^{\infty} V_m^{\text{odd}}(\sigma^z)]^-$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{odd}}(\sigma^z)]^+$	$\|0\rangle\langle 0\|$
3	$[\bigoplus_{m=0}^{\infty} V_m^{\text{odd}}(\sigma^x)]^-$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{odd}}(\sigma^x)]^+$	$\|0\rangle\langle 0\|$

Table 6.2: Alice's ideal measurements. The entry in cell x, a is the projector $\Pi_{A_x}^a$.

y \ b	0	1	2
0	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma_\alpha^z)]^+$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma_\alpha^z)]^-$	0
1	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma_\alpha^x)]^+$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma_\alpha^x)]^-$	0
2	$[\bigoplus_{m=0}^{\infty} V_m^{\text{odd}}(\sigma_\alpha^z)]^-$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{odd}}(\sigma_\alpha^z)]^+$	$\|0\rangle\langle 0\|$
3	$[\bigoplus_{m=0}^{\infty} V_m^{\text{odd}}(\sigma_\alpha^x)]^-$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{odd}}(\sigma_\alpha^x)]^+$	$\|0\rangle\langle 0\|$
4	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma^z)]^+$	$[\bigoplus_{m=0}^{\infty} V_m^{\text{even}}(\sigma^z)]^-$	0

Table 6.3: Bob's ideal measurements. The entry in cell y, b is the projector $\Pi_{B_y}^b$.

Intuitively, for questions $x, y \in \{0,1\}$, Alice and Bob decompose the space into a direct sum of 2×2 blocks and perform the ideal tilted CHSH measurements for ration α on each block. For $x, y \in \{2,3\}$, they do the same, but with a block structure which is shifted forward by one standard basis element. Additionally, Bob has a fifth question on which he performs the same measurement as Alice performs on question $x = 0$.

The ideal state and measurements defining p^* specify correlation tables T_{xy} for all pairs of questions $x \in \{0,1,2,3\}$, $y \in \{0,1,2,3,4\}$. We explicitly report some of them, as we will later make use of the relations that these impose on the measurement projectors. For ease of notation let $C = \frac{1}{1-\alpha^2}$ in the tables below (note $C > 1$).

Table 6.4: On the left, T_{xy} for $x, y \in \{0,1\}$. The top-left 2×2 block contains ideal tilted CHSH correlations for questions x, y.

a \ b	0	1	2
0	$\text{CHSH}^{\alpha}_{x,y}$		0
1			0
2	0	0	0

a \ b	1	0	2
1	$\frac{C-1}{C} \cdot \text{CHSH}^{\alpha}_{\bar{x},\bar{y}}$		0
0			0
2	0	0	$\frac{1}{C}$

Table 6.5: On the right, T_{xy} for $x, y \in \{2,3\}$. Let $\bar{x}, \bar{y}$ be x, y modulo 2. The top-left 2×2 block contains the ideal tilted CHSH correlation table for questions $\bar{x}, \bar{y}$, weighted by $\frac{C-1}{C}$ (notice that we have flipped the 0 and 1 labels in the rows and columns.)

Table 6.6: On the left, T_{xy} for $x = 0, y = 4$

a \ b	0	1	2
0	$\frac{1}{C} \cdot \frac{1}{1-\alpha^4}$	0	0
1	0	$\frac{1}{C} \cdot \frac{\alpha^2}{1-\alpha^4}$	0
2	0	0	0

a \ b	0	1	2
0	$\frac{1}{C} \cdot (\frac{1}{1-\alpha^4} - 1)$	0	0
1	0	$\frac{1}{C} \cdot \frac{\alpha^2}{1-\alpha^4}$	0
2	$\frac{1}{C}$	0	0

Table 6.7: On the right, T_{xy} for $x = 2, y = 4$

6.1.6 Proof of separation

In this section, we prove Theorem 21. We start from a (finite-dimensional) strategy that induces p^*: in Subsection 6.1.6.1, we prove properties of the state and the measurement operators, and in Subsection 6.1.6.2, we characterize the non-zero Schmidt coefficients, concluding that there must be infinitely many (thus giving a contradiction).

6.1.6.1 Characterizing the state and the projectors

The following lemma establishes the existence of two local isometries which decompose any state achieving p^* into two different ways (as anticipated in the proof overview of Section 6.1.2).

Lemma 45 (Characterizing the state and projectors)**.** *Let $(|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{\Pi^a_{A_x}\}, \{\Pi^b_{B_y}\})$ be a strategy inducing the ideal correlation p^* from Definition 39. Let $C = \frac{1}{1-\alpha^2}$. Then there exist two local isometries Φ and Φ' and (normalized) states $|aux\rangle$, $|aux'\rangle$ and $|aux''\rangle$ such that*

(i)
- $\Phi(|\psi\rangle) = \frac{1}{\sqrt{1+\alpha^2}}(|00\rangle + \alpha\,|11\rangle) \otimes |aux\rangle$
- $\Phi(\Pi^0_{A_0} \otimes I\,|\psi\rangle) = \frac{1}{\sqrt{1+\alpha^2}}\,|00\rangle \otimes |aux\rangle$
- $\Phi(\Pi^1_{A_0} \otimes I\,|\psi\rangle) = \frac{\alpha}{\sqrt{1+\alpha^2}}\,|11\rangle \otimes |aux\rangle$

(ii)
- $\Phi'(|\psi\rangle) = \frac{1}{\sqrt{C}}\,|22\rangle \otimes |aux''\rangle \oplus \sqrt{\frac{C-1}{C}}\frac{1}{\sqrt{1+\alpha^2}}(|11\rangle + \alpha\,|00\rangle) \otimes |aux'\rangle$
- $\Phi'(\Pi^0_{A_2} \otimes I\,|\psi\rangle) = \sqrt{\frac{C-1}{C}}\frac{\alpha}{\sqrt{1+\alpha^2}}\,|00\rangle \otimes |aux'\rangle$
- $\Phi'(\Pi^1_{A_2} \otimes I\,|\psi\rangle) = \sqrt{\frac{C-1}{C}}\frac{1}{\sqrt{1+\alpha^2}}\,|11\rangle \otimes |aux'\rangle$
- $\Phi'(\Pi^2_{A_2} \otimes I\,|\psi\rangle) = \frac{1}{\sqrt{C}}\,|22\rangle \otimes |aux''\rangle$.

Proof. (i): Let p' be the restriction of p^* to questions $x, y \in \{0,1\}$. From Table 6.4, we know that p' is the ideal tilted CHSH correlation for ratio α (except that it has an extra answer "2" which has zero probability mass). Applying the block decomposition lemma (Lemma 44) with $\omega_1 = 1$ and $\omega_2 = 0$, we have that there exist subspaces $\mathcal{H}^1_A \subseteq \mathcal{H}_A$ and $\mathcal{H}^1_B \subseteq \mathcal{H}_B$ such that the strategy $(|\psi\rangle \in \mathcal{H}^1_A \otimes \mathcal{H}^1_B, \{\Pi^a_{A_x}|_{\mathcal{H}^1_A}\}_{a\in\{0,1\}}, \{\Pi^b_{B_y}|_{\mathcal{H}^1_B}\}_{b\in\{0,1\}})$ induces the ideal tilted CHSH correlation.

By Lemma 43, the tilted CHSH correlation self-tests its ideal strategy, i.e. there exists a local isometry $\Phi_1 = \Phi_{1,A} \otimes \Phi_{1,B}$ with $\Phi_{1,A} : \mathcal{H}^1_A \to \tilde{\mathcal{H}}^1_A \otimes \tilde{\mathcal{H}}^1_{A,aux}$ and $\Phi_{1,B} : \mathcal{H}^1_B \to \tilde{\mathcal{H}}^1_B \otimes \tilde{\mathcal{H}}^1_{B,aux}$, and a (normalized) state $|aux\rangle \in \tilde{\mathcal{H}}^1_{A,aux} \otimes \tilde{\mathcal{H}}^1_{B,aux}$ such that $\Phi_1(|\psi\rangle) = \frac{1}{\sqrt{1+\alpha^2}}(|00\rangle + \alpha\,|11\rangle) \otimes |aux\rangle$. Moreover, by Lemma 43, it is also the case that

$$\Phi_1\left((\Pi^0_{A_0}|_{\mathcal{H}^1_A} - \Pi^1_{A_0}|_{\mathcal{H}^1_A}) \otimes I\,|\psi\rangle\right) = Z \otimes I\frac{1}{\sqrt{1+\alpha^2}}(|00\rangle + \alpha\,|11\rangle) \otimes |aux\rangle\,.$$

Since $(I+Z)/2 = |0\rangle\langle 0|$ and $(I-Z)/2 = |1\rangle\langle 1|$, we deduce by linearity that

$$\Phi_1\left(\Pi^0_{A_0}|_{\mathcal{H}^1_A} \otimes I\,|\psi\rangle\right) = \frac{1}{\sqrt{1+\alpha^2}}\,|00\rangle \otimes |aux\rangle \text{ and } \Phi_1\left(\Pi^1_{A_0}|_{\mathcal{H}^1_A} \otimes I\,|\psi\rangle\right) = \frac{\alpha}{\sqrt{1+\alpha^2}}\,|11\rangle \otimes |aux\rangle\,.$$

Letting Φ be any isometric extension of Φ_1 to $\mathcal{H}_A \otimes \mathcal{H}_B$ and applying condition (iv) of Lemma 44 gives (i).

(ii): Let p'' be the restriction of p^* to questions $x, y \in \{2,3\}$. Then from table 6.5 we have that $p'' = \omega_1 p_1 \oplus \omega_2 p_2$ where p_1 is the ideal tilted CHSH correlation (for ratio α) and p_2 is the correlation in which answer $(2,2)$ has probability 1 on all question pairs, and $\omega_1 = \frac{C-1}{C}$, $\omega_2 = \frac{1}{C}$.

By Lemma 44, there exist subspaces $\mathcal{H}_A^{\text{null}}, \mathcal{H}_B^{\text{null}}, \mathcal{H}_A^1, \mathcal{H}_A^2, \mathcal{H}_B^1, \mathcal{H}_B^2$ with $\mathcal{H}_A = \mathcal{H}_A^{\text{null}} \oplus \mathcal{H}_A^1 \oplus \mathcal{H}_A^2$ and $\mathcal{H}_B = \mathcal{H}_B^{\text{null}} \oplus \mathcal{H}_B^1 \oplus \mathcal{H}_B^2$, and strategies S_1 and S_2 with

$$S_1 = \left(\frac{|\psi_1\rangle}{\| |\psi\rangle \|} \in \mathcal{H}_A^1 \otimes \mathcal{H}_B^1, \{\Pi_{A_x}^a|_{\mathcal{H}_A^1}\}_{a\in\{0,1\}}, \{\Pi_{B_y}^b|_{\mathcal{H}_B^1}\}_{b\in\{0,1\}} \right),$$
$$S_2 = \left(\frac{|\psi_2\rangle}{\| |\psi_2\rangle \|} \in \mathcal{H}_A^2 \otimes \mathcal{H}_B^2, \{\Pi_{A_x}^2|_{\mathcal{H}_A^2}\}, \{\Pi_{B_y}^2|_{\mathcal{H}_B^2}\} \right)$$

such that $\| |\psi_1\rangle \|^2 = \frac{C-1}{C}$, $\| |\psi_2\rangle \|^2 = \frac{1}{C}$ and $|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle$. Moreover, S_1 induces the ideal tilted CHSH correlation for ratio α (with the roles of the 0 and 1 answers flipped — see Table 6.5). As in the proof of (i), we can apply Lemma 43 to obtain local isometries $\Phi_1 = \Phi_{1,A} \otimes \Phi_{1,B}$ with $\Phi_{1,A} : \mathcal{H}_A^1 \to \tilde{\mathcal{H}}_A^1 \otimes \tilde{\mathcal{H}}_{A,aux}^1$ and $\Phi_{1,B} : \mathcal{H}_B^1 \to \tilde{\mathcal{H}}_B^1 \otimes \tilde{\mathcal{H}}_{B,aux}^1$, and a (normalized) state $|aux'\rangle \in \tilde{\mathcal{H}}_{A,aux}^1 \otimes \tilde{\mathcal{H}}_{B,aux}^1$ such that

(a) $\Phi_1(|\psi_1\rangle) = \sqrt{\frac{C-1}{C}} \frac{1}{\sqrt{1+\alpha^2}} (|11\rangle + \alpha |00\rangle) \otimes |aux'\rangle$, (we have flipped the zero and one basis elements for later convenience)

(b) $\Phi_1(\Pi_{A_2}^1|_{\mathcal{H}_A^1} \otimes I |\psi_1\rangle) = \sqrt{\frac{C-1}{C}} \frac{1}{\sqrt{1+\alpha^2}} |11\rangle \otimes |aux'\rangle$, and

(c) $\Phi_1(\Pi_{A_2}^0|_{\mathcal{H}_A^1} \otimes I |\psi_1\rangle) = \sqrt{\frac{C-1}{C}} \frac{\alpha}{\sqrt{1+\alpha^2}} |00\rangle \otimes |aux'\rangle$,

where (b) and (c) are obtained similarly as in part (i) of this proof.

Now, let $\Phi_2 = \Phi_{2,A} \otimes \Phi_{2,B}$, with $\Phi_{2,A} : \mathcal{H}_A^2 \to \tilde{\mathcal{H}}_A^2 \otimes \tilde{\mathcal{H}}_{A,aux}^2$ and $\Phi_{2,B} : \mathcal{H}_B^2 \to \tilde{\mathcal{H}}_B^2 \otimes \tilde{\mathcal{H}}_{B,aux}^2$ be a local isometry, and $|aux''\rangle \in \tilde{\mathcal{H}}_{A,aux}^2 \otimes \tilde{\mathcal{H}}_{B,aux}^2$ a (normalized) state such that

(d) $\Phi_2(|\psi_2\rangle) = \frac{1}{\sqrt{C}} |22\rangle \otimes |aux''\rangle$.

Such Φ_2 and $|aux''\rangle$ trivially exist.

Define

- $\Phi'_A : \mathcal{H}_A^1 \oplus \mathcal{H}_A^2 \to (\tilde{\mathcal{H}}_A^{(1)} \otimes \tilde{\mathcal{H}}_{A,aux}^{(1)}) \oplus (\tilde{\mathcal{H}}_A^{(2)} \otimes \tilde{\mathcal{H}}_{A,aux}^{(2)})$ as $\Phi'_A = \Phi_{1,A} \oplus \Phi_{2,A}$
- $\Phi'_B : \mathcal{H}_B^1 \oplus \mathcal{H}_B^2 \to (\tilde{\mathcal{H}}_B^{(1)} \otimes \tilde{\mathcal{H}}_{B,aux}^{(1)}) \oplus (\tilde{\mathcal{H}}_B^{(2)} \otimes \tilde{\mathcal{H}}_{B,aux}^{(2)})$ as $\Phi'_B = \Phi_{1,B} \oplus \Phi_{2,B}$

Let Φ''_A be any isometric extension of Φ'_A to $\mathcal{H}_A$, and let Φ''_B be any isometric extension of Φ'_B to $\mathcal{H}'_B$. Let $\Phi' = \Phi''_A \otimes \Phi''_B$. Then (a), (b), (c) and (d), together with condition (iv) of Lemma 44, imply that Φ' satisfies condition (ii) of Lemma 45, as desired.

□

We also need the following properties, obtained using the $y = 4$ question on Bob's side.

Lemma 46. *Let* $(|\psi\rangle, \{\Pi^a_{A_x}\}, \{\Pi^b_{B_y}\})$ *be a strategy inducing* p^*. *The following properties hold:*

(i) $\Pi^0_{A_0}|\psi\rangle = \Pi^0_{B_4}|\psi\rangle = (\Pi^2_{A_2} + \Pi^0_{A_2})|\psi\rangle$

(ii) $\Pi^1_{A_0}|\psi\rangle = \Pi^1_{B_4}|\psi\rangle = \Pi^1_{A_2}|\psi\rangle$

(iii) $|\psi\rangle = \Pi^0_{A_0} \otimes \Pi^0_{B_4}|\psi\rangle + \Pi^1_{A_0} \otimes \Pi^1_{B_4}|\psi\rangle$.

Proof. From correlation table 6.6, we read out that $\langle\psi|\Pi^0_{A_0}\Pi^0_{B_4}|\psi\rangle = \|\Pi^0_{A_0}|\psi\rangle\|^2 = \|\Pi^0_{B_4}|\psi\rangle\|^2$. By the Cauchy-Schwarz inequality, this implies that $\Pi^0_{A_0}|\psi\rangle = \Pi^0_{B_4}|\psi\rangle$. Similarly, from correlation table 5.7, we deduce $(\Pi^2_{A_2} + \Pi^0_{A_2})|\psi\rangle = \Pi^0_{B_4}|\psi\rangle$, which yields (i). We derive (ii) analogously. Item (iii) follows from combining the previous two items with the equality $(\Pi^0_{A_0} + \Pi^1_{A_0})|\psi\rangle = |\psi\rangle$. □

6.1.6.2 Characterizing the Schmidt coefficients

From now onwards, let $(|\psi\rangle, \{\Pi^a_{A_x}\}, \{\Pi^b_{B_y}\})$ be a strategy inducing p^*. In the previous subsection, we gave a partial characterization of the operators and state. In this subsection, we make use of these properties to show that $|\psi\rangle$ must have infinitely many Schmidt coefficients, and therefore deduce that any strategy inducing the separating correlation defined in Subsection 6.1.5 must be infinite-dimensional.

For a bipartite state $|\phi\rangle_{AB}$, we denote by $\mathrm{Sch}(|\phi\rangle_{AB})$ the multiset[1] of non-zero Schmidt coefficients of $|\phi\rangle_{AB}$. Recall that the Schmidt coefficients $\{\lambda_i\}$ are the unique nonnegative real numbers so that $|\phi\rangle_{AB} = \sum_i \lambda_i |i\rangle_A \otimes |i\rangle_B$ for some bases of the A and B registers. Any such pair of bases is called a pair of *Schmidt bases with respect to* $|\phi\rangle$. Usually the tensor product decomposition of the Hilbert space will be clear, in which case we'll simply write $\mathrm{Sch}(|\phi\rangle)$ without the subscripts. We will use the following basic fact about Schmidt coefficients; we provide a proof for completeness.

Lemma 47. *Let* $|\psi\rangle, |\phi\rangle, |\eta\rangle$ *be states on* $\mathcal{H}_A \otimes \mathcal{H}_B$ *with* $|\psi\rangle = |\phi\rangle + |\eta\rangle$. *Define reduced densities*

$$\rho_A = \mathrm{Tr}_B |\psi\rangle\langle\psi|, \sigma_A = \mathrm{Tr}_B |\phi\rangle\langle\phi|, \tau_A = \mathrm{Tr}_B |\eta\rangle\langle\eta|$$

on $\mathcal{H}_A$. *Define* ρ_B, σ_B, τ_B *similarly. Suppose that* $|\phi\rangle$ *and* $|\eta\rangle$ *are "orthogonal on both subsystems" in the sense that* $\sigma_A\tau_A = 0 = \sigma_B\tau_B$. *Then* $\mathrm{Sch}(|\psi\rangle) = \mathrm{Sch}(|\phi\rangle) \sqcup \mathrm{Sch}(|\eta\rangle)$, *where* $\sqcup$ *denotes disjoint union.*

[1] Here by multiset we mean a set with multiplicity, sometimes called an unordered list. For example, the multiset of Schmidt coefficients of the EPR pair is $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$.

Proof. A Schmidt basis for $\mathcal{H}_A$ with respect to $|\psi\rangle$ is the same as an eigenbasis for the reduced density operator $\mathrm{Tr}_B |\psi\rangle\langle\psi|$. Using the orthogonality of $|\phi\rangle$ and $|\eta\rangle$, one can check that the three densities ρ_A, σ_A, τ_A commute. Therefore, the densities have a common eigenbasis. This is also a common Schmidt basis. After repeating the argument to find a common Schmidt basis on $\mathcal{H}_B$, we can write the states as

$$|\psi\rangle = \sum_i \lambda_i |ii\rangle\,, |\phi\rangle = \sum_i a_i |ii\rangle\,, \text{ and } |\eta\rangle = \sum_i b_i |ii\rangle\,,$$

with $a_i + b_i = \lambda_i$. By the orthogonality of $|\eta\rangle$ and $|\phi\rangle$, we have $a_i b_i = 0$ for each i. This implies that for each i, exactly one of the following two equalities holds: $\lambda_i = a_i$ or $\lambda_i = b_i$. This yields the lemma. □

Lemma 48. *Let Φ, Φ' and $|aux\rangle$, $|aux'\rangle$, $|aux''\rangle$ be the local isometries and auxiliary states from Lemma 45. Let $S = \mathrm{Sch}(|\psi\rangle)$, and let $S_2 = \mathrm{Sch}\left(\frac{1}{\sqrt{C}} |22\rangle \otimes |aux''\rangle\right)$. Then there exists a partition $S = S_0 \sqcup S_1$ such that:*

- $S_0 = \mathrm{Sch}\left(\frac{1}{\sqrt{1+\alpha^2}} |00\rangle \otimes |aux\rangle\right) = S_2 \sqcup \mathrm{Sch}\left(\sqrt{\frac{C-1}{C}} \frac{\alpha}{\sqrt{1+\alpha^2}} |00\rangle \otimes |aux'\rangle\right)$
- $S_1 = \mathrm{Sch}\left(\frac{\alpha}{\sqrt{1+\alpha^2}} |11\rangle \otimes |aux\rangle\right) = \mathrm{Sch}\left(\sqrt{\frac{C-1}{C}} \frac{1}{\sqrt{1+\alpha^2}} |11\rangle \otimes |aux'\rangle\right)$

Notice that these two equalities give us two different correspondences between the Schmidt coefficients of $|aux\rangle$ and $|aux'\rangle$, where one involves multiplying by α and the other involves dividing by α.

Proof. Recall from Lemma 46 that $|\psi\rangle = \Pi^0_{A_0} \otimes \Pi^0_{B_4} |\psi\rangle + \Pi^1_{A_0} \otimes \Pi^1_{B_4} |\psi\rangle$. We deduce by Lemma 47 that S can be partitioned into two sets S_0 and S_1, where

$$S_0 = \mathrm{Sch}\left(\Pi^0_{A_0} |\psi\rangle\right) \text{ and } S_1 = \mathrm{Sch}\left(\Pi^1_{A_0} |\psi\rangle\right). \tag{6.12}$$

Since local isometries preserve Schmidt coefficients, $\Phi(|\psi\rangle)$, $\Phi'(|\psi\rangle)$ and $|\psi\rangle$ have the same set of Schmidt coefficients S. Moreover, Lemma 45 gives

$$\Phi(\Pi^0_{A_0} |\psi\rangle) = \frac{1}{\sqrt{1+\alpha^2}} |00\rangle \otimes |aux\rangle \text{ and } \Phi(\Pi^1_{A_0} |\psi\rangle) = \frac{\alpha}{\sqrt{1+\alpha^2}} |11\rangle \otimes |aux\rangle\,.$$

By direct substitution,

$$S_0 = \mathrm{Sch}\left(\frac{1}{\sqrt{1+\alpha^2}} |00\rangle \otimes |aux\rangle\right) \text{ and } S_1 = \mathrm{Sch}\left(\frac{\alpha}{\sqrt{1+\alpha^2}} |11\rangle \otimes |aux\rangle\right).$$

By Lemma 46, we also have $\Pi^0_{A_0}|\psi\rangle = (\Pi^2_{A_2} + \Pi^0_{A_2})|\psi\rangle$ and $\Pi^1_{A_0}|\psi\rangle = \Pi^1_{A_2}|\psi\rangle$. Moreover, from Lemma 45, we also have $\Phi'((\Pi^2_{A_2} + \Pi^0_{A_2})|\psi\rangle) = \frac{1}{\sqrt{C}}|22\rangle \otimes |aux''\rangle + \sqrt{\frac{C-1}{C}}\frac{\alpha}{\sqrt{1+\alpha^2}}|00\rangle \otimes |aux'\rangle$ and $\Phi'(\Pi^1_{A_2}|\psi\rangle) = \sqrt{\frac{C-1}{C}}\frac{1}{\sqrt{1+\alpha^2}}|11\rangle \otimes |aux'\rangle$. Then this implies

$$\begin{aligned} S_0 &= \mathrm{Sch}\left(\frac{1}{\sqrt{C}}|22\rangle \otimes |aux''\rangle + \sqrt{\frac{C-1}{C}}\frac{\alpha}{\sqrt{1+\alpha^2}}|00\rangle \otimes |aux'\rangle\right) \\ &= S_2 \sqcup \mathrm{Sch}\left(\sqrt{\frac{C-1}{C}}\frac{\alpha}{\sqrt{1+\alpha^2}}|00\rangle \otimes |aux'\rangle\right), \text{ and} \\ S_1 &= \mathrm{Sch}\left(\sqrt{\frac{C-1}{C}}\frac{1}{\sqrt{1+\alpha^2}}|11\rangle \otimes |aux'\rangle\right). \end{aligned} \tag{6.13}$$

Putting together Equations (6.12) through (6.13) gives the statement of the Lemma. □

Theorem 22. *Let p^* be the ideal correlation introduced in Definition 39. Let $(|\psi\rangle, \{\Pi^a_{A_x}\}, \{\Pi^b_{B_y}\})$ be any strategy inducing p^*. Then $|\psi\rangle$ has infinitely many non-zero Schmidt coefficients.*

Proof. Let $|aux\rangle, |aux'\rangle$, S_0, S_1 and S_2 be as in Lemma 48. Recall from Lemma 48 that

$$S_0 = \mathrm{Sch}\left(\frac{1}{\sqrt{1+\alpha^2}}|00\rangle \otimes |aux\rangle\right) \text{ and } S_1 = \mathrm{Sch}\left(\frac{\alpha}{\sqrt{1+\alpha^2}}|11\rangle \otimes |aux\rangle\right).$$

Then we can rewrite these sets as

$$S_0 = \left\{\frac{1}{\sqrt{1+\alpha^2}}\lambda : \lambda \in \mathrm{Sch}(|aux\rangle)\right\} \text{ and } S_1 = \left\{\frac{1}{\sqrt{1+\alpha^2}}\alpha\lambda : \lambda \in \mathrm{Sch}(|aux\rangle)\right\}.$$

Notice that there is a bijection $f : S_0 \to S_1$ such that $f(\lambda) = \alpha\lambda$. Again from Lemma 48 we have

$$S_0 = S_2 \sqcup \mathrm{Sch}\left(\sqrt{\frac{C-1}{C}}\frac{\alpha}{\sqrt{1+\alpha^2}}|00\rangle \otimes |aux'\rangle\right) \text{ and } S_1 = \mathrm{Sch}\left(\sqrt{\frac{C-1}{C}}\frac{1}{\sqrt{1+\alpha^2}}|11\rangle \otimes |aux'\rangle\right).$$

Then we can rewrite $S_0 \setminus S_2$ and S_1 as

$$\begin{aligned} S_0 \setminus S_2 &= \left\{\sqrt{\frac{C-1}{C}}\frac{\alpha}{\sqrt{1+\alpha^2}}\lambda : \lambda \in \mathrm{Sch}(|aux'\rangle)\right\} \text{ and} \\ S_1 &= \left\{\sqrt{\frac{C-1}{C}}\frac{1}{\sqrt{1+\alpha^2}}\lambda : \lambda \in \mathrm{Sch}(|aux'\rangle)\right\}. \end{aligned}$$

Notice that there is a bijection $g : S_1 \to S_0 \setminus S_2$ such that $g(\lambda) = \alpha\lambda$.

Composing the maps f and g yields a bijection between S_0 and $S_0 \setminus S_2$. Since S_2 is nonempty, this implies that S_0 must be infinite. □

One can extend this proof a bit farther. Repeated applications of the map $f \circ g$ show that S_0 has an infinite descending sequence of the form $(\lambda, \alpha^2\lambda, \alpha^4\lambda, \ldots)$. One more application f then shows that S has an infinite sequence $(\lambda, \alpha\lambda, \alpha^2\lambda, \alpha^3\lambda, \ldots)$ This can be used to obtain some quantitative bounds on the dimension required to induce a correlation close to the ideal one. We do not prove this quantitative bound because much more useful bounds already exist for correlations witnessing the separation $\mathcal{C}_{qs} \neq \mathcal{C}_{qa}$.

6.2 Non-closure of the set of quantum correlations: an elementary proof from self-testing and embezzlement

6.2.1 Introduction

We started our journey by discovering Bell's theorem [9], which asserts that there exist games for which players who share entanglement can outperform players who do not, the most famous example being the CHSH game [17]. The most immediate application of non-local games is to "test quantumness": a referee who observes a winning probability in a non-local game which exceeds what is attainable classically can have high confidence that the players (or devices) she is interacting with were sharing entanglement. As we have seen throughout this thesis, a more refined analysis of non-local games allows the referee to obtain more precise characterizations of the devices involved. In many cases, it is possible for the referee to obtain almost-exact characterizations of the devices.

In this work, we take a step back, and we focus on the study of non-local games as witnesses of high-dimensional entanglement. In other words, we are interested not necessarily in characterizing a quantum device fully, but just in certifying that the associated quantum system has at least a certain dimension. The study of *dimension witnesses* has had on the one hand fruitful applications in quantum cryptography, and on the other it has shed light on basic questions in the theory of entanglement.

6.2.1.1 Certifying high-dimensional entanglement - previous work and state of the art

Non-local games with the property that a near-optimal score provides a lower bound on the dimension of the players' quantum systems are referred to as *dimension witnesses*. The study of games (or correlations) with such a property was initiated by Brunner et al. [13], who coined the term. In this work, we focus on dimension witnesses that can certify entanglement of arbitrarily high dimension.

The first example of a game which cannot be won perfectly with any finite amount of entanglement was proposed by Leung, Toner and Watrous [53], and is intimately connected to our result. The game that they introduced is not a non-local game in the usual sense, since it involves *quantum* questions and answers. However, it has the property that in order to succeed with high probability, the players have to perform a coherent state exchange which requires them to share an embezzling state of high dimension. More precisely, the game forces the two players to coherently transform a product state of two qubits into an EPR pair, using only local operations. This task is, of course, impossible to perform exactly, but can be performed to arbitrarily high precision if the two players share an auxiliary entangled state of sufficiently high dimension (referred to as an *embezzling* state).

Subsequently, several examples of dimension witnesses for entanglement of arbitrarily high dimension have been proposed over the years consisting of non-local games with classical questions

and answers [10, 88, 12, 57, 16, 29, 22, 24, 69, 25]. However, all of these examples involve *families* of non-local games whose questions and answers increase as the witnessed dimension increases. For some time, it was an open question to determine whether there exists a non-local game, with a finite number of questions and answers, whose optimal value cannot be attained by any finite-dimensional strategy (in the tensor product model), but which can be attained in the limit of finite-dimensional strategies. This question was answered recently by Slofstra in a sequence of two breakthrough works [90, 89], where he introduces novel techniques based on the representation theory of finitely-presented groups. Slofstra's result implies that the set of quantum correlations is not closed.

An alternative proof of the latter result was given subsequently by Dykema, Paulsen, and Prakash [33], and more recently by Musat and Rørdam [68], using techniques based on the representation theory of C^*-algebras. The games constructed in [33] and [68] have significantly smaller question and answer set sizes, namely 5 and 2.

In contrast, the result that we described in Section 6.1 gives an example of a point in the set of quantum correlations on question sets of size 5 and answer sets of size 3 which cannot be attained using finite-dimensional entanglement but *can* be attained exactly using infinite-dimensional entanglement, in the tensor product model. This asserts that the the set $\mathcal{C}_q$ of quantum correlations attainable with finite-dimensional entanglement is strictly contained in the set $\mathcal{C}_{qs}$ of correlations attainable with possibly infinite-dimensional entanglement.

All of the above results are not explicit or quantitative about the tradeoff between winning probability (or expected score in the game) and the dimension required to attain it. What we desire from a dimension witness is a quantitative statement of the following form: if the players' score is ϵ-close to optimal, then their strategy has dimension at least $f(\epsilon)$, where $f(\epsilon)$ is a function that tends to infinity as ϵ tends to zero. In [91], Slofstra and Vidick analyze such a tradeoff for the machinery introduced by Slofstra in [90], and they relate such tradeoff to a quantity called the *hyperlinear profile* of a group. In a subsequent work [87], Slofstra provides a finitely-presented group whose hyperlinear profile is at least subexponential. As a corollary, this yields a two-player non-local game, with question and answer sets of finite size, with the property that a $1-\epsilon$ winning probability requires dimension at least $2^{\Omega(\epsilon^{-c})}$ to attain for some constant $0 < c < 1$. The caveat of such a non-local game is that its description is quite involved and the size of question and answer sets is large. Moreover, it is not clear whether a winning probability of 1 in the game can be attained in the limit of finite-dimensional strategies or not (although it can be attained in the commuting-operator model). These caveats not only make an experimental demonstration of such a dimension witness infeasible, but, more importantly, they somewhat conceal what is truly happening behind the scenes: the resulting non-local game, although remarkable for its behaviour, does not arguably

provide much intuition about what is causing the exponential blow-up of the dimension.

A much simpler game with a similar exponential tradeoff between optimality and dimension, and without this caveat, but involving three players, was proposed recently by Ji, Leung and Vidick [50]. Their work constitutes, in some sense, a return to the original ideas of Leung, Toner and Watrous'coherent state-exchange game [53], which are cleverly translated to a setting in which all questions and answers are classical. At the heart of the three-player non-local game of Ji, Leung and Vidick is the idea of delegating the actions of the *quantum* verifier of the coherent state-exchange game to a third player. By combining different non-local tests, the verifier is still able, using only classical communication, to enforce that two of the three players must be performing a coherent state-exchange which involves a high-dimensional embezzling state as a resource.

6.2.1.2 Our result

In this work, we show, strikingly, that the third player is not required. We design a much more direct two-player non-local game with an (improved) exponential trade-off between optimality and dimension: one of the key ideas is the introduction of a simple additional sub-test which can guarantee the coherence of a state-exchange between the two players even in the absence of a "physical" third register that forces coherence, like in the games of [53] and [50]. Our result is the following:

Theorem 23. *(informal) There exists a two-player non-local game on question sets of size* 5 *and* 6*, and answer sets of size* 3*, with the property that:*

- *(completeness) For any* $\epsilon > 0$*, there exists a strategy of dimension* $2^{O(\epsilon^{-1})}$ *that is* ϵ*-close to optimal.*
- *(soundness) Any* ϵ*-close to optimal strategy has at least* $2^{\Omega(\epsilon^{-1/8})}$ *dimension.*

Our game can be thought of as a direct *de-quantization* of the coherent state-exchange game. It is by far the simplest non-local game (in terms of question and answer set size) with such an exponential tradeoff. For a comparison, even with three players, the question and answer sets are of size 12 and 8 respectively in [50].

Our game provides a new proof of the non-closure of the set of quantum correlations. However, strikingly, compared to the proofs in [89], [33] and [68], our proof is arguably elementary, and does not involve any representation-theoretic machinery. We point out, additionally, that an exponential tradeoff between optimality and dimension does not hold for the game in [33], where a strategy of

dimension $1/poly(\epsilon)$ can be ϵ-close to optimal (and we suspect that this is also the case for the game in [68]).

Next, we sketch the main ideas in the design of our two-player non-local game.

6.2.1.3 A sketch of our two-player non-local game

Our game consists of sub-tests (a), (b) and (c), executed by the verifier with equal probability:

(a) A non-local game $G_{\text{3-CHSH}}$ whose unique optimal strategy requires the provers to share the state $|00\rangle + |11\rangle + |22\rangle$. $G_{\text{3-CHSH}}$ is an instance (for $d = 3$) of a more general family of non-local games from [21]. $G_{\text{3-CHSH}}$ contains a special "computational basis" question for Alice which requires her to measure her half of the state in the computational basis.

(b) The well-known "tilted CHSH" non-local game, which we denote by G_{tCHSH} [1, 7]. This requires, for the appropriate choice of parameters, that the provers share the state $|00\rangle + \sqrt{2}\,|11\rangle$. G_{tCHSH} contains a special "computational basis" question for Bob, which requires him to measure in the computational basis.

(c) A sub-test in which Alice is asked the "computational basis" question from (a), and Bob is asked the "computational basis" question from (b). Alice and Bob win if: either they both answer "0", or they both answer different from "0".

The intuition behind the game is the following: Alice and Bob could share the state $(|00\rangle + |11\rangle + |22\rangle)_{\mathsf{AB}} \otimes (|00\rangle + \sqrt{2}\,|11\rangle)_{\mathsf{A'B'}}$. This would allow them to win parts (a) and (b) optimally, but they would fail in part (c). The power of part (c) is that Alice is uncertain about whether she is being asked a question from part (a) or (c), and Bob is uncertain about whether he is being asked a question from part (b) or (c). Magically, the condition of part (c) is sufficient to enforce that Alice and Bob cannot keep the two optimal states from part (a) and (b) into two separate registers, but rather they should coherently transform one into the other in order to achieve consistency in answering part (c). This coherent transformation is what requires an exponentially growing amount of entanglement dimension to perform to increasing precision. We refer the reader to Section 6.2.4 for a formal description of our game.

Organization Section 6.2.2 reviews two non-local games which are used as sub-tests in our non-local game. Section 6.2.3 briefly introduces embezzlement. Section 6.2.4 describes our non-local game. Section 6.2.5 covers completeness: we give a family of strategies that approximates arbitrarily well the optimal value in our non-local game. Section 6.2.6 covers soundness: we show

that any close to optimal strategy requires high-dimensional entanglement. Section 6.2.7 briefly discusses how our non-local game implies the non-closure of the set of quantum correlations.

6.2.2 Two sub-tests

In this section, we review the two non-local games which we will employ as sub-tests in our non-local game.

Tilted CHSH We have already introduced the tilted CHSH inequality in Section 3.4. For the purposes of the current section, we will recast tilted CHSH as a non-local game (recall that Bell inequalitied and non-local games are equivalent. Here we make this equivalence explicit). First, we will recall here, for convenience, the form of the ideal strategy for tilted CHSH.

The maximum in the tilted CHSH inequality is attained by the following strategy:

Definition 40 (Ideal strategy for tilted CHSH)**.** *Given parameter $\beta \in [0,2)$, let $\theta \in (0, \frac{\pi}{4}]$ be such that $\sin 2\theta = \sqrt{\frac{4-\beta^2}{4+\beta^2}}$, $\mu = \arctan \sin 2\theta$, and $\alpha = \tan\theta$. Define the α-*tilted Pauli operators *as*

$$\sigma_\alpha^z := \cos\mu\sigma^z + \sin\mu\sigma^x, \text{ and } \sigma_\alpha^x := \cos\mu\sigma^z - \sin\mu\sigma^x.$$

The ideal strategy for tilted CHSH with parameter β (i.e. achieving maximal violation of (3.14)*) consists of the joint state $|\Psi\rangle = \cos\theta(|00\rangle + \alpha|11\rangle)$ and observables A_0, A_1 and B_0, B_1 with $A_0 = \sigma^z$, $A_1 = \sigma^x$, $B_0 = \sigma_\alpha^z$ and $B_1 = \sigma_\alpha^x$.*

β and α are related by an invertible function, and α is typically the parameter of interest, so we choose to denote by $\mathrm{tCHSH}(\alpha)$ the tilted CHSH game whose ideal state is $|\Psi\rangle = \cos\theta(|00\rangle + \alpha|11\rangle)$.

We can equivalently formulate the tilted CHSH inequality as a non-local game, as follows:

Definition 41 (Tilted CHSH as a non-local game)**.** *For $\alpha \in (0,1]$, the tilted CHSH game $G_{\mathrm{tCHSH}(\alpha)}$ is*

$$G_{\mathrm{tCHSH}(\alpha)} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, D, V_{\mathrm{tCHSH}(\alpha)}),$$

where $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B} = \{0,1\}$, D is uniform on $\mathcal{X} \times \mathcal{Y}$, and $V_{\mathrm{tCHSH}(\alpha)} = (-1)^{a\oplus b - xy} + \delta_{\{x=y=0\}} \cdot \beta \cdot (-1)^a$, where β and α are related as in Definition 40.

Proposition 5 (Quantum value of the tilted CHSH game)**.** *For $\alpha \in (0,1]$, the value of $G_{\mathrm{tCHSH}(\alpha)}$ is $\omega^*_{\mathrm{tCHSH}(\alpha)} := \frac{1}{4} \cdot \sqrt{8+2\beta^2}$, where β and α are related as in Definition 40.*

Proof. Notice that for any strategy S, the value $\omega(S, G_{\mathrm{tCHSH}}(\alpha))$ takes precisely the form of the LHS of (3.14) (upon associating, for each observable in (3.14), the projection onto the $+1$-eigenspace with answer 0 and the projection onto the -1-eigenspace with answer 1, and up to a factor of $\frac{1}{4}$ from sampling the questions uniformly). □

In other words, the LHS of the tilted CHSH inequality and the value of the tilted CHSH game are equivalent reformulations of one another. The following theorem asserts a robust self-testing result for tilted CHSH, i.e. that any strategy that attains a value close to the quantum value of the game, must be close to the ideal strategy of Definition 40 (in the following statement we only write down the conditions that we make use of later).

Theorem 24 (Self-testing with tilted CHSH ([102, 7]))**.** *Let $\alpha \in (0,1]$. Maximal value in $G_{\mathrm{tCHSH}(\alpha)}$ self-tests the ideal strategy of Definition 40 with robustness $O(\sqrt{\epsilon})$, i.e. for any strategy $S = (|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{P_x^a\}, \{Q_y^b\})$ with value $\omega(S, G_{\mathrm{tCHSH}(\alpha)}) > \omega^*_{\mathrm{tCHSH}(\alpha)} - \epsilon$ there exists a local isometry V and an auxiliary state $|aux\rangle$ such that:*

- $|\Psi\rangle \approx_{V, O(\epsilon^{1/2})} \frac{1}{\sqrt{1+\alpha^2}}(|00\rangle + \alpha\,|11\rangle) \otimes |aux\rangle$
- $P_0^0\,|\Psi\rangle \approx_{V, O(\epsilon^{1/2})} \frac{1}{\sqrt{1+\alpha^2}}\,|00\rangle \otimes |aux\rangle$

The last condition means that the first player's measurement on question "0" is equivalent (up to a change of basis) to a computational basis measurement.

For clarity of notation and exposition in later sections, it is convenient for us to define the game $G_{\sim\mathrm{tCHSH}(\alpha)}$, for $\alpha \in (0,1]$. This is an equivalent version of $G_{\mathrm{tCHSH}(\alpha)}$ with the only difference that the scoring function is $V_{\sim\mathrm{tCHSH}(\alpha)} := (-1)^{a\oplus b - xy} - \delta_{\{x=y=0\}} \cdot \beta \cdot (-1)^a$ (notice the minus sign). It is easy to see that this game is equivalent to the original tilted CHSH up to a flip of the answer labels (so in particular $\omega^*_{\mathrm{tCHSH}(\alpha)} = \omega^*_{\sim\mathrm{tCHSH}(\alpha)}$). The corresponding version of Theorem 24 for $G_{\sim\mathrm{tCHSH}(\alpha)}$ is as follows:

Theorem 25. *Let $\alpha \in (0,1]$. Maximal value in $G_{\sim\mathrm{tCHSH}(\alpha)}$ self-tests the ideal strategy of Definition 40 with robustness $O(\sqrt{\epsilon})$, i.e. for any strategy $S = (|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{P_x^a\}, \{Q_y^b\})$ with value $\omega(S, G_{\sim\mathrm{tCHSH}(\alpha)}) > \omega^*_{\sim\mathrm{tCHSH}(\alpha)} - \epsilon$ there exists a local unitary V and an auxiliary state $|aux\rangle$ such that:*

- $|\Psi\rangle \approx_{V, O(\epsilon^{1/2})} \frac{1}{\sqrt{1+\alpha^2}}(\alpha\,|00\rangle + |11\rangle) \otimes |aux\rangle$
- $P_0^0\,|\Psi\rangle \approx_{V, O(\epsilon^{1/2})} \frac{\alpha}{\sqrt{1+\alpha^2}}\,|00\rangle \otimes |aux\rangle$

Generalization of CHSH self-testing states of local dimension d In Section 5.2, we introduced a family of Bell inequalities, or non-local games, parametrized by $d \geq 2 \in \mathbb{N}$, which generalizes the CHSH game [21]. For convenience, we recall here the essential properties of this family which we will need in this section. The games in this family have the property that, for the game with parameter d, maximal score in the game self-tests the maximally entangled state of local dimension

d. Each of the games in this family is a 2-player game in which question sets are of size $2 + \mathbb{1}_{d>2}$ and $2 + 2 \cdot \mathbb{1}_{d>2}$, and answer sets are of size d. When $d = 2$, the game coincides with the usual CHSH game. We denote by $G_{d\text{-CHSH}}$ the game in the family with parameter d. We do not describe this family of games in full detail here (for details we refer to [21]). We will just recall the self-testing properties of the game that we need in the following theorem, and describe the ideal strategy for the case of $d = 3$ (we will use $G_{3\text{-CHSH}}$ later as a sub-test in our non-local game).

Theorem 26 ([21])**.** *There exists a family of non-local games $\{G_{d\text{-CHSH}}\}_{d\geq 2\in\mathbb{N}}$ with the following properties:*

- *Question sets are:*
  - $\mathcal{X} = \mathcal{Y} = \{0,1\}$, *for* $d = 2$
  - $\mathcal{X} = \{0,1,2\}, \mathcal{Y} = \{0,1,2,3\}$, *for* $d > 2$.

  Answer sets are $\mathcal{A} = \mathcal{B} = \{0,1,..,d-1\}$. For all d, the distribution over questions is uniform. Denote by $V_{d\text{-CHSH}}$ the scoring function for $G_{d\text{-CHSH}}$.
- *(Self-testing) Let $\omega^*_{d\text{-CHSH}}$ be the value of the game with parameter d. There exists a constant $C > 0$ such that the following holds. Any strategy $S = (|\Psi\rangle, \{P^a_x\}, \{Q^b_y\})$ with value $\omega(S, G_{d\text{-CHSH}}) \geq \omega^*_{d\text{-CHSH}} - \epsilon$, for some $0 < \epsilon < \frac{C}{d^3}$, is such that there exists a local unitary V and an auxiliary state $|aux\rangle$ such that:*
  - $|\Psi\rangle \approx_{V, O(d^6\epsilon^{1/8})} \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle \otimes |aux\rangle$
  - $P^i_0 |\Psi\rangle \approx_{V, O(d^6\epsilon^{1/8})} \frac{1}{\sqrt{d}} |ii\rangle \otimes |aux\rangle$.

Again, the last condition means that the first player's measurement on question "0" is equivalent (up to a change of basis) to a computational basis measurement.

Next, we describe the ideal strategy for $G_{3\text{-CHSH}}$. First, we fix some notation.

We define an isometry $V : (\mathbb{C}^2)_A \to (\mathbb{C}^3)_{\tilde{A}}$ as follows:

$$V|0\rangle = |1\rangle, \quad V|1\rangle = |2\rangle$$

For an operator O on $\mathbb{C}^2$, we write $V(O)$ to refer to the pushforward $VOV^\dagger$ of O along V. For example, $V(\sigma^z) = |1\rangle\langle 1| - |2\rangle\langle 2|$. If O has $+1, 0, -1$ eigenvalues, we write O^+ for the projection onto the $+1$ eigenspace and O^- for the projection onto the -1 eigenspace. One can check that with this notation $O = O^+ - O^-$. We use the notation $\bigoplus A_i$ to denote the direct sum of observables A_i. If $\mathcal{H}_A \approx \mathbb{C}^3$, we still write σ^z_A to mean $\sigma^z_A = |0\rangle\langle 0|_A - |1\rangle\langle 1|_A$. On the other

hand, in accordance with the notation above, we write $V(\sigma^z)_A$ to mean $V(\sigma^z)_A = |1\rangle\langle 1| - |2\rangle\langle 2|$. We adopt an analogous notation for all other Paulis and tilted Paulis, and projections onto their eigenspaces. (We will make use of the α-tilted Paulis $\sigma^z_\alpha, \sigma^x_\alpha$ from Definition 40).

Definition 42 (Ideal strategy for $G_{\text{3-CHSH}}$ [21])**.** *The ideal strategy for $G_{\text{3-CHSH}}$ is $(|\Psi\rangle, \{P^a_x\}, \{Q^b_y\})$, where $|\Psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$, and the ideal measurements are described in Tables 6.8 and 6.9.*

x \ a	0	1	2
0	$\|0\rangle\langle 0\|_{\tilde{A}}$	$\|1\rangle\langle 1\|_{\tilde{A}}$	$\|2\rangle\langle 2\|_{\tilde{A}}$
1	$(\sigma^x)^+$	$(\sigma^x)^-$	$\|2\rangle\langle 2\|$
2	$\|0\rangle\langle 0\|$	$[V(\sigma^x)]^+$	$[V(\sigma^x)]^-$

Table 6.8: Alice's ideal measurements for $G_{\text{3-CHSH}}$. The entry in cell x, a is the projector P^a_x.

y \ b	0	1	2
0	$(\sigma^z_{\alpha=1})^+$	$(\sigma^z_{\alpha=1})^-$	$\|2\rangle\langle 2\|$
1	$(\sigma^x_{\alpha=1})^+$	$(\sigma^x_{\alpha=1})^-$	$\|2\rangle\langle 2\|$
2	$\|0\rangle\langle 0\|$	$[V(\sigma^z_{\alpha=1})]^+$	$[V(\sigma^z_{\alpha=1})]^-$
3	$\|0\rangle\langle 0\|$	$[V(\sigma^x_{\alpha=1})]^+$	$[V(\sigma^x_{\alpha=1})]^-$

Table 6.9: Bob's ideal measurements for $G_{\text{3-CHSH}}$. The entry in cell y, b is the projector P^b_y.

We emphasize, as it will be important later, that both the ideal strategies for $G_{\text{tCHSH}(\alpha)}$ and $G_{d\text{-CHSH}}$ include a computational basis measurement for the first player on question "0".

6.2.3 Embezzlement

The phenomenon of *embezzlement* was first discovered by van Dam and Hayden [30]. A family of embezzling states can be used to coherently transform a product state into an EPR pair (or viceversa). The fidelity of this transformation increases with the dimension of the embezzling state.

Definition 43 (Embezzlement)**.** *Let $\{|\Gamma_d\rangle\}_{d\in\mathbb{N}}$ be a collection of states, where $|\Gamma_d\rangle \in (\mathbb{C}^2)^{\otimes d}_{A'} \otimes (\mathbb{C}^2)^{\otimes d}_{B'}$. We say that $\{|\Gamma_d\rangle\}_{d\in\mathbb{N}}$ is an "embezzling family" if there exist unitaries $W_{AA'}$ on $\mathbb{C}^2_A \otimes (\mathbb{C}^2)^{\otimes d}_{A'}$ and $W_{BB'}$ on $\mathbb{C}^2_B \otimes (\mathbb{C}^2)^{\otimes d}_{B'}$ such that*

$$\|W_{AA'} \otimes W_{BB'} |\text{EPR}\rangle_{AB} |\Gamma_d\rangle_{A'B'} - |11\rangle_{AB} |\Gamma_d\rangle_{A'B'}\| = O\left(\frac{1}{\sqrt{d}}\right).$$

Example 7. *Let* $|\Gamma_d\rangle = \frac{1}{\sqrt{N_d}} \sum_{j=1}^{d} |11\rangle_{A'B'}^{\otimes j} |\mathrm{EPR}\rangle_{A'B'}^{\otimes(d-j)}$*, where* N_d *is a normalizing constant. Then, the family of states* $\{|\Gamma_d\rangle\}$ *is an embezzling family. The unitaries* $W_{AA'}$ *and* $W_{BB'}$ *are the "left-shift" unitaries, which act on* $\mathbb{C}_A^2 \otimes (\mathbb{C}^2)_{A'}^{\otimes d}$ *and* $\mathbb{C}_B^2 \otimes (\mathbb{C}^2)_{B'}^{\otimes d}$ *respectively, by shifting by one to the left each of the* $d+1$ *qubit registers. It is easy to check that the family of states* $\{|\Gamma_d\rangle\}_{d\in\mathbb{N}}$ *satisfies Definition 43.*

6.2.4 The non-local game

The following is our non-local game. We describe it informally first, and then we give a precise description in Fig. 6.1. We refer to Alice and Bob as the two players in our non-local game.

The non-local game consists of three tests, run with equal probability.

(a) In the first test, the verifier sends both players questions from the game $G_{\text{3-CHSH}}$, and they obtain a score according to its scoring function.

(b) In the second test, the verifier sends both players questions from the (flipped) tilted CHSH game $G_{\sim\text{tCHSH}}(\frac{1}{\sqrt{2}})$. Importantly, their roles are also switched: Alice is sent the questions of player 2 in $G_{\sim\text{tCHSH}}(\frac{1}{\sqrt{2}})$, and Bob the questions of player 1. They obtain a score according to the scoring function of $G_{\sim\text{tCHSH}}(\frac{1}{\sqrt{2}})$.

(c) In the third test, Alice receives the "computational basis" question (question "0" of the first player) from the game $G_{\text{3-CHSH}}$, and Bob receives the "computational basis" question (question "0" of the first player) from the game $G_{\sim\text{tCHSH}}(\frac{1}{\sqrt{2}})$. The players' score is 1 if: Alice answers 0 if and only if Bob answers 0. They score 0 otherwise.

The intuition behind this game is the following.

If Alice and Bob's strategy attains an ϵ-close to optimal expected score overall (where optimally here means playing perfectly in all three tests), then it must attain a 3ϵ-close to optimal expected score in each of the three tests. By the self-testing result of Theorem 26, in order to play 3ϵ-close to optimally in (a), the players need to be sharing a state close to a maximally entangled state of qutrits, up to a local isometry, and moreover one of Alice's measurements is a "computational basis" measurement. By Theorem 25, in order to play 3ϵ-close to optimally in (b), Alice and Bob must be measuring a state close to a tilted EPR pair with ratio $\frac{1}{\sqrt{2}}$, up to a local isometry. Moreover one of Bob's measurements must be a "computational basis" measurement. Crucially, Alice cannot distinguish her question in (c) from a "computational basis" question in (a), while Bob cannot distinguish his question in (c) from a "computational basis" question in (b). In order to play close to optimally in (c), Alice and Bob's computational basis measurements need to satisfy

a consistency condition. It is this consistency condition that forces the two players to "agree" on a computational basis element $|00\rangle \in \mathbb{C}^3_A \otimes \mathbb{C}^3_B$, and to perform a coherent state exchange such that:

$$\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)_{AB} \mapsto \frac{1}{\sqrt{3}}(|00\rangle + \sqrt{2}\,|11\rangle)_{AB}, \tag{6.14}$$

with $|00\rangle_{AB} \mapsto |00\rangle_{AB}$ and $\frac{1}{\sqrt{2}}(|11\rangle + |22\rangle)_{AB} \mapsto |11\rangle_{AB}$. The LHS of (6.14) is the state that the players need in order to play part (a) perfectly, while the RHS is the state that they need to play part (b) perfectly. Part (c) ensures that players have to "agree" on the term $|00\rangle$, and this enforces that they must perform coherently the exchange in (6.14) to high accuracy if they are to perform well in all three parts.

Next, we give a precise description of our non-local game G_{emb}. We denote by V_{emb} its scoring function. Recall that $V_{\text{3-CHSH}}$ and $V_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})}$ are the scoring functions for games $G_{\text{3-CHSH}}$ and $G_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})}$ respectively.

Question sets: $\mathcal{X} := \Big(\{\text{"3-CHSH"}\} \times \{0,1,2\}\Big) \cup \Big(\{\text{"}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{"}\} \times \{0,1\}\Big)$, and $\mathcal{Y} := \Big(\{\text{"3-CHSH"}\} \times \{0,1,2,3\}\Big) \cup \Big(\{\text{"}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{"}\} \times \{0,1\}\Big)$. Answer sets: $\mathcal{A} = \mathcal{B} = \{0,1,2\}$.

The game consists of the following three parts, executed with equal probability.

(a) Pick uniformly random $x' \in \{0,1,2\}$ and $y' \in \{0,1,2,3\}$. Send $x = (\text{"3-CHSH"}, x')$ to Alice and $y = (\text{"3-CHSH"}, y')$ to Bob. Let a and b be the players' answers. The players' score is $V_{emb}(a,b,x,y) = V_{\text{3-CHSH}}(a,b,x',y')$.

(b) Pick uniformly random $x' \in \{0,1\}$ and $y' \in \{0,1\}$. Send $x = (\text{"}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{"}, x')$ to Alice and $y = (\text{"}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{"}, y')$ to Bob. Let a and b be the players' answers. The players' score is $V_{emb}(a,b,x,y) = V_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})}(b,a,y',x')$ (notice that the roles of the two players is switched in the last expression).

(c) Send question $x = (\text{"3-CHSH"}, 0)$ to Alice, and question $y = (\text{"}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{"}, 0)$ to Bob. Let a and b be the players' answers. Their score is

$$V(a,b,x,y) = \begin{cases} 1, & \text{if } (a,b) \in \{(0,0)\} \cup (\{1,2\} \times \{1,2\}) \\ 0, & \text{otherwise} \end{cases}$$

Figure 6.1: Our non-local game G_{emb}

Proposition 6. *The value of the non-local game G_{emb} of Fig. 6.1 is $\omega^*(G_{emb}) = \frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1)$.*

Proof. Clearly, $\omega^* \leq \frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1)$. Otherwise, there would exist a strategy S such that the value $\omega(S, G_{emb}) > \frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1)$. This would imply that at least one of the following holds:

- The restriction of S to part (a) has value greater than $\omega^*_{\text{3-CHSH}}$.
- The restriction of S to part (b) has value greater than $\omega^*_{\sim\text{tCHSH}}$.
- The restriction of S to part (c) has value greater than 1.

All three of the above are clearly impossible.

On the other hand, we will construct in the next section a sequence of strategies whose value in G gets arbitrarily close to $\frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1)$. This completes the proof. □

6.2.5 Completeness

In this section, we describe a family of strategies whose value in our non-local game G_{emb} gets arbitrarily close to $\frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1)$ (which also completes the proof of Proposition 6). A strategy in the family is parametrized by $d \in \mathbb{N}$. The provers start with the state

$$\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)_{\tilde{A}\tilde{B}} \otimes |\Gamma_d\rangle_{A'B'}\,, \tag{6.15}$$

where $|\Gamma_d\rangle$ is an embezzling state. We give first an informal description of the ideal measurements, and we follow this by a formal description.

- Upon receiving a question with prefix "3-CHSH", Alice and Bob perform the corresponding ideal measurement for 3-CHSH. In particular on question $(\text{"3-CHSH"}, 0)$, Alice measures her half of the state in (6.15) in the computational basis.
- Upon receiving a question with prefix "$\sim$tCHSH($\frac{1}{\sqrt{2}}$)", Alice and Bob first apply embezzling unitaries $W_{\tilde{A}A'}$ and $W_{\tilde{B}B'}$ respectively, such that (approximately) $\frac{1}{\sqrt{2}}(|11\rangle + |22\rangle) \mapsto |11\rangle$ and $|00\rangle \mapsto |00\rangle$. So the resulting state is

$$\sqrt{\frac{2}{3}}\left(\frac{1}{\sqrt{2}}|00\rangle + |11\rangle\right)_{\tilde{A}\tilde{B}} \otimes |\Gamma_d\rangle_{A'B'}\,. \tag{6.16}$$

  They then perform the corresponding ideal measurements for $\sim$tCHSH($\frac{1}{\sqrt{2}}$) on registers $\tilde{A}, \tilde{B}$ (where Alice takes the role of the second player, and Bob takes the role of the first player). In particular, on question $(\text{"}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{"}, 0)$, Bob measures his half of the state in (6.16) in the computational basis.

A key observation is that when Alice and Bob are asked questions $(\text{“3-CHSH”}, 0)$ and $(\text{“}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{”}, 0)$ respectively, then it is straightforward to see that, if they follow the above strategy, they reply with answers (a, b) which attain a score of 1 in part (c) of Fig. 6.1, i.e. $(a, b) \in \{(0,0)\} \cup (\{1,2\} \times \{1,2\})$.

Next, we define the players' ideal measurements precisely. Recall the isometry $V : \mathbb{C}^2 \to \mathbb{C}^3$ defined in Subsection 6.2.2 as follows:

$$V|0\rangle = |1\rangle, \quad V|1\rangle = |2\rangle$$

Recall also the notation introduced in Subsection 6.2.2 along with V. In particular, we write $V(O)$ to refer to the pushforward $VOV^\dagger$ of O along V. For O an operator with $+1, 0, -1$ eigenvalues, we write O^+ for the projection onto the $+1$ eigenspace and O^- for the projection onto the -1 eigenspace. If $\mathcal{H}_A \approx \mathbb{C}^3$, we still write σ^z_A to mean $\sigma^z_A = |0\rangle\langle 0|_A - |1\rangle\langle 1|_A$. On the other hand, in accordance with the notation above, we write $V(\sigma^z)_A$ to mean $V(\sigma^z)_A = |1\rangle\langle 1|_A - |2\rangle\langle 2|_A$.

Let $\{|\Gamma_d\rangle_{ABA'B'}\}$ be the embezzling family from Example 7, and $W_{AA'} : (\mathbb{C}^2)_A \otimes (\mathbb{C}^2)^{\otimes d}_{A'} \to (\mathbb{C}^2)_A \otimes (\mathbb{C}^2)^{\otimes d}_{A'}$, $W_{BB'} : (\mathbb{C}^2)_B \otimes (\mathbb{C}^2)^{\otimes d}_{B'} \to (\mathbb{C}^2)_A \otimes (\mathbb{C}^2)^{\otimes d}_{A'}$ be the left-shift unitaries over the $d+1$ qubit registers. Define $\tilde{W}_{\tilde{A}A'} : (\mathbb{C}^3)_{\tilde{A}} \otimes (\mathbb{C}^2)^{\otimes d}_{A'} \to (\mathbb{C}^3)_{\tilde{A}} \otimes (\mathbb{C}^2)^{\otimes d}_{A'}$ as

$$\tilde{W}_{\tilde{A}A'} = (|0\rangle\langle 0|_{\tilde{A}} \otimes I_{A'}) \oplus [(V \otimes I) W_{AA'} (V^\dagger \otimes I)],$$

and define $\tilde{W}_{\tilde{B}B'}$ analogously.

The following is the family of ideal strategies for G_{emb} achieving a value arbitrarily close to $\frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1)$.

Definition 44 (Ideal strategy for G_{emb})**.** *The family of ideal strategies is* $\{S_d\}_{d\in\mathbb{N}}$*, with* $S_d = (|\Psi_d\rangle, \{P^a_x\}, \{Q^b_y\})$*, where*

$$|\Psi_d\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)_{\tilde{A}\tilde{B}} \otimes |\Gamma_d\rangle_{A'B'},$$

and the ideal measurements are described in Tables 6.10 and 6.11.

x \ a	0	1	2
(“3-CHSH”, 0)	$\|0\rangle\langle 0\|_{\tilde{A}}$	$\|1\rangle\langle 1\|_{\tilde{A}}$	$\|2\rangle\langle 2\|_{\tilde{A}}$
(“3-CHSH”, 1)	$(\sigma^x)^+_{\tilde{A}}$	$(\sigma^x)^-_{\tilde{A}}$	$\|2\rangle\langle 2\|_{\tilde{A}}$
(“3-CHSH”, 2)	$\|0\rangle\langle 0\|_{\tilde{A}}$	$[V(\sigma^x)]^+_{\tilde{A}}$	$[V(\sigma^x)]^-_{\tilde{A}}$
(“tCHSH($\frac{1}{\sqrt{2}}$), 0)	$W^\dagger_{\tilde{A}A'}([\sigma^x(\sigma^z_{\alpha=\frac{1}{\sqrt{2}}})^-\sigma^x]_{\tilde{A}}\otimes I_{A'})W_{\tilde{A}A'}$	$W^\dagger_{\tilde{A}A'}([\sigma^x(\sigma^z_{\alpha=\frac{1}{\sqrt{2}}})^+\sigma^x]_{\tilde{A}}\otimes I_{A'})W_{\tilde{A}A'}$	P_{rest}
(“tCHSH($\frac{1}{\sqrt{2}}$), 1)	$W^\dagger_{\tilde{A}A'}([\sigma^x(\sigma^x_{\alpha=\frac{1}{\sqrt{2}}})^-\sigma^x]_{\tilde{A}}\otimes I_{A'})W_{\tilde{A}A'}$	$W^\dagger_{\tilde{A}A'}([\sigma^x(\sigma^x_{\alpha=\frac{1}{\sqrt{2}}})^+\sigma^x]_{\tilde{A}}\otimes I_{A'})W_{\tilde{A}A'}$	P_{rest}

Table 6.10: Alice's ideal measurements for G_{emb}. The entry in cell x, a is the projector P^a_x (tensored identities are implied where omitted, and P_{rest} completes the set of orthogonal projections in a row).

y \ b	0	1	2
(“3-CHSH”, 0)	$(\sigma^z_{\alpha=1})^+_{\tilde{B}}$	$(\sigma^z_{\alpha=1})^-_{\tilde{B}}$	$\|2\rangle\langle 2\|_{\tilde{B}}$
(“3-CHSH”, 1)	$(\sigma^x_{\alpha=1})^+_{\tilde{B}}$	$(\sigma^x_{\alpha=1})^-_{\tilde{B}}$	$\|2\rangle\langle 2\|_{\tilde{B}}$
(“3-CHSH”, 2)	$\|0\rangle\langle 0\|_{\tilde{B}}$	$[V(\sigma^z_{\alpha=1})]^+_{\tilde{B}}$	$[V(\sigma^z_{\alpha=1})]^-_{\tilde{B}}$
(“3-CHSH”, 3)	$\|0\rangle\langle 0\|_{\tilde{B}}$	$[V(\sigma^x_{\alpha=1})]^+_{\tilde{B}}$	$[V(\sigma^x_{\alpha=1})]^-_{\tilde{B}}$
(“tCHSH($\frac{1}{\sqrt{2}}$), 0)	$W^\dagger_{\tilde{B}B'}([\sigma^x(\sigma^z)^-\sigma^x]_{\tilde{B}}\otimes I_{B'})W_{\tilde{B}B'}$	$W^\dagger_{\tilde{B}B'}([\sigma^x(\sigma^z)^+\sigma^x]_{\tilde{B}}\otimes I_{B'})W_{\tilde{B}B'}$	P_{rest}
(“tCHSH($\frac{1}{\sqrt{2}}$), 1)	$W^\dagger_{\tilde{B}B'}([\sigma^x(\sigma^x)^-\sigma^x]_{\tilde{B}}\otimes I_{B'})W_{\tilde{B}B'}$	$W^\dagger_{\tilde{B}B'}([\sigma^x(\sigma^x)^+\sigma^x]_{\tilde{B}}\otimes I_{B'})W_{\tilde{B}B'}$	P_{rest}

Table 6.11: Bob's ideal measurements for G_{emb}. The entry in cell y, b is the projector P^b_y (tensored identities are implied where omitted, and P_{rest} completes the set of orthogonal projections in a row).

Proposition 7 (Completeness)**.** *Let $\{S_d\}_{d\in\mathbb{N}}$ be the family of strategies from Definition 44, and G_{emb} the non-local game from Fig. 6.1. Then, $\omega(S_d, G_{emb}) = \omega^*(G_{emb}) - O(\frac{1}{d})$.*

Proof. The value of strategy S_d in part (a) is exactly $\omega^*_{\text{3-CHSH}}$. This is because the starting state is the ideal state for $\omega^*_{\text{3-CHSH}}$ and measurements are the ideal ones from Definition 42. The value in part (b) is $\omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} - O(\frac{1}{d})$. This is because the joint state resulting from the embezzling transformation has fidelity $1 - O(\frac{1}{d})$ with the ideal state for $\sim$tCHSH($\frac{1}{\sqrt{2}}$) (from Theorem 25), and the measurements for part (b) are also ideal. The value in part (c) is easily seen to be exactly 1. Thus, $\omega(S_d, G_{emb}) = \frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1) - O(\frac{1}{d})$. Together with the upper bound in the proof of Proposition 6, this completes the proof of Proposition 6

(i.e. $\omega^*(G_{emb}) = \frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1)$), and gives $\omega(S_d, G_{emb}) = \frac{1}{3}(\omega^*_{\text{3-CHSH}} + \omega^*_{\sim\text{tCHSH}(\frac{1}{\sqrt{2}})} + 1) - O(\frac{1}{d})$, as desired. □

6.2.6 Soundness

Theorem 27. *There exists a constant $C > 0$ such that any quantum strategy S for the game G_{emb} of Fig. 6.1 with value $\omega(S, G_{emb}) \geq \omega^*(G_{emb}) - \epsilon$, for some $0 < \epsilon < C$, must have dimension $2^{\Omega(\epsilon^{-1/8})}$.*

The proof of Theorem 27 can be broken down into two parts:

(i) First, we will show that performing well in parts **(a)**, **(b)** and **(c)** of the game imposes a certain structure on the strategy of the provers.

(ii) Second, we show that such a structured strategy can be used to play well also in the "coherent state exchange" game of Leung, Toner, and Watrous [53]. This reduction allows us to translate the lower bounds on the dimension of an approximately optimal strategy in the "coherent state exchange" game to lower bounds on the dimension of an approximately optimal strategy for our game.

Proof of Theorem 27. Let $\left(|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{P^a_x\}, \{Q^b_y\}\right)$ be a strategy whose value in G_{emb} is ϵ-close to $\omega^*(G_{emb}) = \frac{1}{3}(w^*_{\text{3CHSH}} + w^*_{\text{2CHSH}} + 1)$. This implies that, for each part of the game, the strategy's expected score is 3ϵ-close to optimal. From each part, we deduce the following consequences. Note that these hold also for infinite-dimensional strategies (on separable Hilbert spaces), since the self-testing results we invoke also do.

(a) From Theorem 26 (the case $d = 3$), upon picking an appropriate constant $C > 0$, there exists a local isometry $\Phi : \mathcal{H}_A \otimes \mathcal{H}_B \to (\mathbb{C}^3)_{A_1} \otimes (\mathbb{C}^3)_{B_1} \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$, and an auxiliary state $|aux\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ such that

- $|\psi\rangle \approx_{\Phi, O(\epsilon^{1/8})} \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle) \otimes |aux\rangle$
- $P^0_{(\text{"3-CHSH"},0)} |\psi\rangle \approx_{\Phi, O(\epsilon^{1/8})} \frac{1}{\sqrt{3}} |00\rangle \otimes |aux\rangle$

(b) From Theorem 25, there exists a local isometry $\Phi' : \mathcal{H}_A \otimes \mathcal{H}_B \to (\mathbb{C}^2)_{A_2} \otimes (\mathbb{C}^2)_{B_2} \otimes \mathcal{H}_{A''} \otimes \mathcal{H}_{B''}$, and an auxiliary state $|aux'\rangle \in \mathcal{H}_{A''} \otimes \mathcal{H}_{B''}$ such that

- $|\psi\rangle \approx_{\Phi', O(\epsilon^{1/2})} \frac{1}{\sqrt{3}}(|00\rangle + \sqrt{2}\,|11\rangle) \otimes |aux'\rangle$
- $Q^0_{(\text{"}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{"},0)} |\psi\rangle \approx_{\Phi', O(\epsilon^{1/2})} \frac{1}{\sqrt{3}} |00\rangle \otimes |aux'\rangle$

(c) $P^0_{(\text{“3-CHSH”},0)}\,|\psi\rangle \approx_{O(\epsilon^{1/2})} Q^0_{(\text{“}\sim\text{tCHSH}(\frac{1}{\sqrt{2}})\text{”},0)}\,|\psi\rangle$

Notice that **(a), (b), (c)** $\Rightarrow$ the local isometry $\tilde{\Phi} := (\Phi')(\Phi)^\dagger : (\mathbb{C}^3)_{A_1} \otimes (\mathbb{C}^3)_{B_1} \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \rightarrow (\mathbb{C}^2)_{A_2} \otimes (\mathbb{C}^2)_{B_2} \otimes \mathcal{H}_{A''} \otimes \mathcal{H}_{B''}$ is such that

$$\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle) \otimes |aux\rangle \approx_{\tilde{\Phi},O(\epsilon^{1/8})} \frac{1}{\sqrt{3}}(|00\rangle + \sqrt{2}\,|11\rangle) \otimes |aux'\rangle\,, \tag{6.17}$$

and moreover

$$\frac{1}{\sqrt{3}}\,|00\rangle \otimes |aux\rangle \approx_{\tilde{\Phi},O(\epsilon^{1/8})} \frac{1}{\sqrt{3}}\,|00\rangle \otimes |aux'\rangle\,. \tag{6.18}$$

(6.17) and (6.18) immediately imply that

$$\frac{1}{\sqrt{2}}(|11\rangle + |22\rangle) \otimes |aux\rangle \approx_{\tilde{\Phi},O(\epsilon^{1/8})} |11\rangle \otimes |aux'\rangle\,. \tag{6.19}$$

We claim that the local isometry $\tilde{\Phi}$ can be used to approximately win the “coherent state exchange” game of Leung, Toner and Watrous [53]. More precisely, since Equation (6.19) is $O(\epsilon^{1/8})$-approximate (with respect to Euclidean norm), we claim that one can construct a strategy which employs $\tilde{\Phi}$, and in which the provers' initial state is $|aux\rangle$, which wins the game of [53] with probability $1 - O(\epsilon^{1/4})$. Assuming this claim is true, the rest of the proof is straightforward: it was shown in [53] that the winning probability of any strategy in the “coherent state exchange game” is upper bounded by $1 - \frac{1}{32\log^2(3d)}$, where d is the dimension of the states used; this implies that it must be

$$\frac{1}{32\log^2(3d)} = O(\epsilon^{1/4}) \Rightarrow d = 2^{\Omega(\epsilon^{-\frac{1}{8}})}.$$

To conclude the proof of Theorem 27, we prove the above claim.

The “coherent state exchange” game of [53] between a quantum referee and two non-communicating provers, proceeds as follows:

- The referee initializes a qubit register R and qutrit registers S and T in the state

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathsf{R}}\,|00\rangle_{\mathsf{ST}} + |1\rangle_{\mathsf{R}}\,|\phi^+\rangle_{\mathsf{ST}}), \tag{6.20}$$

  where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The referee sends registers S and T to Alice and Bob respectively.

- The referee receives single-qubit registers A and B from Alice and Bob respectively. The triple $(\mathsf{R},\mathsf{A},\mathsf{B})$ is measured with projective measurement $\{\Pi_0, \Pi_1\}$, where $\Pi_0 = I - |\gamma\rangle\langle\gamma|$ and $\Pi_1 = |\gamma\rangle\langle\gamma|$, and $|\gamma\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

Consider the following strategy of the provers for this game. They start by sharing the state $|aux\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$. Upon receiving the qutrit registers S and T of the state (6.20), they apply $\tilde{\Phi}$ to registers $(\mathbb{C}^3)_{\mathsf{S}} \otimes (\mathbb{C}^3)_{\mathsf{T}} \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ (up to relabelling registers A_1 and B_1 as S and T), obtaining a state in $(\mathbb{C}^2)_{A_2} \otimes (\mathbb{C}^2)_{B_2} \otimes \mathcal{H}_{A''} \otimes \mathcal{H}_{B''}$. Equations (6.18) and (6.19) imply that the resulting state on registers $\mathsf{R}, A_2, B_2, A'', B''$ is $O(\epsilon^{1/8})$-close to $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes |aux'\rangle$. And hence the state on R, A_2, B_2 is $O(\epsilon^{1/8})$-close to the desired state (in Euclidean norm). Qubit registers A_2 and B_2 are then sent back to the referee as A and B. Converting the $O(\epsilon^{1/8})$-closeness to a probability of winning in the game, gives a lower bound of $1 - O(\epsilon^{1/4})$, and thus concludes the proof.

□

6.2.7 Non-closure of the set of quantum correlations

A corollary of Proposition 7 and Theorem 27 (completeness and soundness for our game) is that the set $\mathcal{C}_{qs}$ of quantum correlations induced by quantum strategies in the tensor product model, on possibly infinite-dimensional and separable Hilbert spaces, is not closed, i.e. $\mathcal{C}_{qs} \neq \mathcal{C}_{qa}$ (see the beginning of Chapter 6 for formal definitions of these sets). We use superscripts to denote question and answer set sizes. For instance, $\mathcal{C}_{qs}^{m,n,r,s}$ is on question sets of size m, n and answer sets of size r, s.

Corollary 7. $\mathcal{C}_{qs}^{5,6,3,3} \neq \mathcal{C}_{qa}^{5,6,3,3}$.

Proof. In the proof of Theorem 27, we argued that any strategy with value $\omega^*(G_{emb}) - \epsilon$ in our game G_{emb} can be used to construct a strategy that embezzles an EPR pair into a product state, up to $O(\epsilon^{1/8})$ error in Euclidean norm. This implies that no strategy has value exactly $\omega^*(G_{emb})$. Suppose otherwise for a contradiction. Then, by the reduction in the proof of Theorem 27, we can construct a strategy that wins the game of [53] with probability 1. From [53], this is known to imply existence of a strategy that embezzles perfectly (the argument that shows this implication in [53] is phrased for finite-dimensional strategies, but it holds also for infinite-dimensional ones). A perfect embezzling strategy consists of a state $|\Psi\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ and a local unitary $U = U_{AA'} \otimes U_{BB'}$ such that $U |\phi^+\rangle_{AB} \otimes |\Psi\rangle_{A'B'} = |00\rangle_{AB} \otimes |\Psi\rangle_{A'B'}$. Since Schmidt coefficients are preserved under local unitaries, it is clear that, whatever the Schmidt coefficients of $|\Psi\rangle$ are, the Schmidt coefficients of the LHS and RHS are different. This gives a contradiction.

On the other hand, Proposition 7 gives a sequence of strategies whose value tends to $\omega^*(G_{emb})$. If one considers the sequence of correlations induced by such strategies, it is clear that such a sequence has a limit, and that the limiting correlation has value $\omega^*(G_{emb})$. Such a limiting correlation is thus in $\mathcal{C}_{qa}^{5,6,3,3}$ but not in $\mathcal{C}_{qs}^{5,6,3,3}$.

□

We emphasize that strictly stronger separations (for question sets of size 5 and answer sets of size 2) are known [33, 68]. The latter appeared after the original breakthrough proof of Slofstra, for much larger question and answer sets [89]. What stands out about our proof is that, unlike all previous proofs, it does not involve any representation-theoretic machinery.

BIBLIOGRAPHY

[1] Antonio Acín, Serge Massar, and Stefano Pironio. "Randomness versus nonlocality and entanglement". In: *Physical Review Letters* 108.10 (2012), p. 100402.

[2] Antonio Acín et al. "Quantum nonlocality in two three-level systems". In: *Physical Review A* 65.5 (2002), p. 052325.

[3] Dorit Aharonov, Michael Ben-Or, and Elad Eban. "Interactive Proofs For Quantum Computations". In: *Proceedings of the first Symposium on Innovations in Computer Science (ICS 2010)*. 2010, pp. 453–469.

[4] Gorjan Alagic et al. "Quantum Fully Homomorphic Encryption With Verification". In: *arXiv preprint arXiv:1708.09156* (2017).

[5] PK Aravind. "Quantum mysteries revisited again". In: *American Journal of Physics* 72.10 (2004), pp. 1303–1307.

[6] Alex Arkhipov. "Extending and characterizing quantum magic games". In: *arXiv preprint arXiv:1209.3819* (2012).

[7] Cédric Bamps and Stefano Pironio. "Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing". In: *Physical Review A* 91.5 (2015), p. 052111.

[8] Mohammad Bavarian and Peter W. Shor. "Information Causality, Szemerédi-Trotter and Algebraic Variants of CHSH". In: *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science* (2015), pp. 123–132.

[9] John S. Bell. "On the Einstein-Podolsky-Rosen Paradox". In: *Physics* 1 (1964), pp. 195–200.

[10] Jop Briët, Harry Buhrman, and Ben Toner. "A generalized Grothendieck inequality and nonlocal correlations that require high entanglement". In: *Communications in mathematical physics* 305.3 (2011), pp. 827–843.

[11] Anne Broadbent. "How to verify a quantum computation". In: *Theory of Computing* 14.11 (2018). arXiv preprint arXiv:1509.09180, pp. 1–37.

[12] Nicolas Brunner, Miguel Navascués, and Tamás Vértesi. "Dimension witnesses and quantum state discrimination". In: *Physical review letters* 110.15 (2013), p. 150501.

[13] Nicolas Brunner et al. "Testing the dimension of Hilbert spaces". In: *Physical review letters* 100.21 (2008), p. 210503.

[14] H. Buhrman and S. Massar. "Causality and Tsirelson's bounds". In: *Phys. Rev. A* 72 (2005), p. 052103.

[15] Yudong Cao et al. "Quantum chemistry in the age of quantum computing". In: *Chemical reviews* 119.19 (2019), pp. 10856–10915.

[16] Rui Chao et al. “Test for a large amount of entanglement, using few measurements”. In: *arXiv preprint arXiv:1610.00771* (2016).

[17] John F Clauser et al. “Proposed experiment to test local hidden-variable theories”. In: *Physical review letters* 23.15 (1969), p. 880.

[18] Richard Cleve, Li Liu, and William Slofstra. “Perfect commuting-operator strategies for linear system games”. In: *arXiv preprint arXiv:1606.02278* (2016).

[19] Richard Cleve and Rajat Mittal. “Characterization of binary constraint system games”. In: *International Colloquium on Automata, Languages, and Programming*. Springer. 2014, pp. 320–331.

[20] Andrea Coladangelo. “A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations”. In: *arXiv preprint arXiv:1904.02350* (2019).

[21] Andrea Coladangelo. “Generalization of the Clauser-Horne-Shimony-Holt inequality self-testing maximally entangled states of any local dimension”. In: *Physical Review A* 98.5 (2018), p. 052115.

[22] Andrea Coladangelo. “Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game”. In: *Quantum Information & Computation* 17.9-10 (2017), pp. 831–865.

[23] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. “All pure bipartite entangled states can be self-tested”. In: *Nature communications* 8 (2017), p. 15485.

[24] Andrea Coladangelo and Jalex Stark. “Robust self-testing for linear constraint system games”. In: *arXiv preprint arXiv:1709.09267* (2017).

[25] Andrea Coladangelo and Jalex Stark. “Separation of finite and infinite-dimensional quantum correlations, with infinite question or answer sets”. In: *arXiv preprint arXiv:1708.06522* (2017).

[26] Andrea Coladangelo and Jalex Stark. “Unconditional separation of finite and infinite-dimensional quantum correlations”. In: *arXiv preprint arXiv:1804.05116* (2018).

[27] Andrea Coladangelo et al. “Verifier-on-a-Leash: New Schemes for Verifiable Delegated Quantum Computation, with Quasilinear Resources”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2019, pp. 247–277.

[28] Daniel Collins et al. “Bell inequalities for arbitrarily high-dimensional systems”. In: *Physical review letters* 88.4 (2002), p. 040404.

[29] Matthew Coudron and Anand Natarajan. “The parallel-repeated magic square game is rigid”. In: *arXiv preprint arXiv:1609.06306* (2016).

[30] Wim van Dam and Patrick Hayden. “Universal entanglement transformations without communication”. In: *Physical Review A* 67.6 (2003), p. 060302.

[31] Yfke Dulek, Christian Schaffner, and Florian Speelman. "Quantum homomorphic encryption for polynomial-sized circuits". In: *Advances in Cryptology – Proceedings of the 36th Annual International Cryptology Conference (CRYPTO 2016)*. arXiv:1603.09717. 2016, pp. 3–32.

[32] David Steven Dummit and Richard M Foote. *Abstract algebra*. Vol. 3. Wiley Hoboken, 2004.

[33] Ken Dykema, Vern I Paulsen, and Jitendra Prakash. "Non-closure of the set of quantum correlations via graphs". In: *Communications in Mathematical Physics* (2017), pp. 1–18.

[34] Kenneth J Dykema and Vern Paulsen. "Synchronous correlation matrices and Connes' embedding conjecture". In: *Journal of Mathematical Physics* 57.1 (2016), p. 015214.

[35] Joseph F. Fitzsimons. *Private quantum computation: An introduction to blind quantum computing and related protocols*. arXiv preprint arXiv:1611.10107. 2016.

[36] Joseph F. Fitzsimons and Michal Hajdušek. *Post hoc verification of quantum computation*. arXiv preprint arXiv:1512.04375. 2015.

[37] Joseph F. Fitzsimons and Elham Kashefi. "Unconditionally verifiable blind quantum computation". In: *Physical Review A* 96.012303 (2017). arXiv preprint arXiv:1203.5217.

[38] M. Froissart. "Constructive generalization of Bell's inequalities". In: *Il Nuovo Cimento B (1971-1996)* 64 (1981), pp. 241–251.

[39] Keisuke Fujii and Masahito Hayashi. "Verifiable fault tolerance in measurement-based quantum computation". In: *Physical Review A* 96 (3 Sept. 2017), p. 030301. DOI: 10.1103/PhysRevA.96.030301. URL: https://link.aps.org/doi/10.1103/PhysRevA.96.030301.

[40] Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. "Robustness and device independence of verifiable blind quantum computing". In: *New Journal of Physics* 17 (2015).

[41] Koon Tong Goh et al. "Geometry of the set of quantum correlations". In: *Physical Review A* 97.2 (2018), p. 022104.

[42] Alex B. Grilo. *Relativistic verifiable delegation of quantum computation*. arXiv preprint arXiv:1711.09585. 2017.

[43] Rudolf Haag and Daniel Kastler. "An algebraic approach to quantum field theory". In: *Journal of Mathematical Physics* 5.7 (1964), pp. 848–861.

[44] Michal Hajdušek, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. *Device-independent verifiable blind quantum computation*. arXiv preprint arXiv:1502.02563. 2015.

[45] Masahito Hayashi and Michal Hajdušek. *Self-guaranteed measurement-based quantum computation*. arXiv preprint arXiv:1603.02195. 2016.

[46] Masahito Hayashi and Tomoyuki Morimae. "Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing". In: *Physical Review Letters* 115 (22 Nov. 2015), p. 220502. DOI: 10.1103/PhysRevLett.115.220502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.115.220502.

[47] He-Liang Huang et al. “Experimental Blind Quantum Computing for a Classical Client”. In: *Physical Review Letters* 119 (5 Aug. 2017), p. 050503.

[48] *IBM Q Experience*. URL: https://www.ibm.com/quantum-computing/technology/experience/.

[49] Zhengfeng Ji. “Classical verification of quantum proofs”. In: *Proceedings of the Forty-eighth Annual ACM SIGACT Symposium on Theory of Computing (STOC 2016)*. 2016, pp. 885–898.

[50] Zhengfeng Ji, Debbie Leung, and Thomas Vidick. “A three-player coherent state embezzlement game”. In: *arXiv preprint arXiv:1802.04926* (2018).

[51] Julia Kempe and Thomas Vidick. “Parallel Repetition of Entangled Games”. In: *arXiv preprint arXiv:1012.4728* (2010).

[52] Emanuel Knill et al. “Randomized benchmarking of quantum gates”. In: *Physical Review A* 77.1 (2008), p. 012307.

[53] Debbie Leung, Ben Toner, and John Watrous. “Coherent state exchange in multi-prover quantum interactive proof systems”. In: *Chicago Journal of Theoretical Computer Science* 11.2013 (2013), p. 1.

[54] Urmila Mahadev. “Classical Homomorphic Encryption for Quantum Circuits”. In: *arXiv preprint arXiv:1708.02130* (2017).

[55] Urmila Mahadev. “Classical Verification of Quantum Computations”. In: *arXiv preprint arXiv:1804.01082* (2018).

[56] Laura Mančinska and Thomas Vidick. “Unbounded entanglement can be needed to achieve the optimal success probability”. In: *International Colloquium on Automata, Languages, and Programming*. Springer. 2014, pp. 835–846.

[57] Laura Mančinska and Thomas Vidick. “Unbounded entanglement in nonlocal games”. In: *International Colloquium on Automata, Languages, and Programming* (2014), pp. 835–846.

[58] Dominic Mayers and Andrew Yao. “Self testing quantum apparatus”. In: *Quantum Information & Computation* 4.4 (2004), pp. 273–286.

[59] Matthew McKague. “Interactive Proofs for BQP via Self-Tested Graph States”. In: *Theory of Computing* 12.3 (2016). arXiv preprint arXiv:1309.5675, pp. 1–42.

[60] Matthew McKague. “Self-testing graph states”. In: *Conference on Quantum Computation, Communication, and Cryptography*. Springer. 2011, pp. 104–120.

[61] Matthew McKague. “Self-testing in parallel”. In: *New Journal of Physics* 18.4 (2016), p. 045013.

[62] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. “Robust self-testing of the singlet”. In: *Journal of Physics A: Mathematical and Theoretical* 45.45 (2012), p. 455304.

[63] N David Mermin. “Simple unified form for the major no-hidden-variables theorems”. In: *Physical Review Letters* 65.27 (1990), p. 3373.

[64] Carl A Miller and Yaoyun Shi. “Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices”. In: *Journal of the ACM (JACM)* 63.4 (2016), p. 33.

[65] Tomoyuki Morimae. “Verification for measurement-only blind quantum computing”. In: *Physical Review A* 89 (2014).

[66] Tomoyuki Morimae and Joseph F. Fitzsimons. *Post hoc verification with a single prover*. arXiv preprint arXiv:1603.06046. 2016.

[67] Tomoyuki Morimae, Yuki Takeuchi, and Masahito Hayashi. *Verified measurement-based quantum computing with hypergraph states*. arXiv:1701.05688. 2017.

[68] Magdalena Musat and Mikael Rørdam. “Non-closure of quantum correlation matrices and factorizable channels that require infinite dimensional ancilla”. In: *arXiv preprint arXiv:1806.10242* (2018).

[69] Anand Natarajan and Thomas Vidick. “A quantum linearity test for robustly verifying entanglement”. In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*. ACM. 2017, pp. 1003–1015.

[70] Anand Natarajan and John Wright. “NEEXP in MIP”. In: *arXiv preprint arXiv:1904.05870* (2019).

[71] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. 2002.

[72] Dimiter Ostrev and Thomas Vidick. “Entanglement of approximate quantum strategies in XOR games”. In: *arXiv preprint arXiv:1609.01652* (2016).

[73] Narutaka Ozawa. “About the Connes embedding conjecture”. In: *Japanese Journal of Mathematics* 8.1 (2013), pp. 147–183.

[74] Károly F. Pál and Tamás Vértesi. “Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems”. In: *Phys. Rev. A* 82 (2 2010), p. 022116.

[75] Károly F Pál, Tamás Vértesi, and Miguel Navascués. “Device-independent tomography of multipartite quantum states”. In: *Phys. Rev. A* 90.4 (2014), p. 042340.

[76] Matteo GA Paris. “Quantum estimation for quantum technology”. In: *International Journal of Quantum Information* 7.supp01 (2009), pp. 125–137.

[77] Vern I Paulsen and Ivan G Todorov. “Quantum chromatic numbers via operator systems”. In: *The Quarterly Journal of Mathematics* 66.2 (2015), pp. 677–692.

[78] Vern I Paulsen et al. “Problems of Tsirelson and Connes, and a hierarchy of combinatorial parameters”. In: (2014).

[79] Asher Peres. “Incompatible results of quantum measurements”. In: *Physics Letters A* 151.3-4 (1990), pp. 107–108.

[80] Sandu Popescu and Daniel Rohrlich. “Which states violate Bell’s inequality maximally?” In: *Physics Letters A* 169.6 (1992), pp. 411–414.

[81] John Preskill. “Lecture notes for physics 229: Quantum information and computation”. In: *California Institute of Technology* 16 (1998).

[82] Ben W Reichardt, Falk Unger, and Umesh Vazirani. “Classical command of quantum systems”. In: *Nature* 496.7446 (2013), p. 456.

[83] Alexia Salavrakos et al. “Bell inequalities for maximally entangled states”. In: *arXiv preprint arXiv:1607.04578* (2016).

[84] Volkher B Scholz and Reinhard F Werner. “Tsirelson’s problem”. In: *arXiv preprint arXiv:0812.4305* (2008).

[85] Peter W Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. In: *SIAM review* 41.2 (1999), pp. 303–332.

[86] Jamie Sikora, Antonios Varvitsiotis, and Zhaohui Wei. “Minimum Dimension of a Hilbert Space Needed to Generate a Quantum Correlation”. In: *Phys. Rev. Lett.* 117 (6 Aug. 2016), p. 060401. DOI: 10.1103/PhysRevLett.117.060401. URL: http://link.aps.org/doi/10.1103/PhysRevLett.117.060401.

[87] William Slofstra. “A group with at least subexponential hyperlinear profile”. In: *arXiv preprint arXiv:1806.05267* (2018).

[88] William Slofstra. “Lower bounds on the entanglement needed to play XOR non-local games”. In: *Journal of Mathematical Physics* 52.10 (2011), p. 102202.

[89] William Slofstra. “The set of quantum correlations is not closed”. In: *Forum of Mathematics, Pi*. Vol. 7. Cambridge University Press. 2019.

[90] William Slofstra. “Tsirelson’s problem and an embedding theorem for groups arising from non-local games”. In: *arXiv preprint arXiv:1606.03140* (2016).

[91] William Slofstra and Thomas Vidick. “Entanglement in non-local games and the hyperlinear profile of groups”. In: *Annales Henri Poincaré*. Vol. 19. 10. Springer. 2018, pp. 2979–3005.

[92] Stephen J Summers and Reinhard Werner. “Maximal violation of Bell’s inequalities is generic in quantum field theory”. In: *Communications in Mathematical Physics* 110.2 (1987), pp. 247–259.

[93] Ivan Šupić and Joseph Bowles. “Self-testing of quantum systems: a review”. In: *arXiv preprint arXiv:1904.10042* (2019).

[94] Armin Tavakoli et al. “Quantum Random Access Codes Using Single d-Level Systems”. In: *Phys. Rev. Lett.* 114 (2015), p. 170502.

[95] B Tsirelson. “Quantum Bell-type inequalities”. In: *Hadronic Journal Supplement* 8 (1993), pp. 329–345.

[96] Umesh Vazirani and Thomas Vidick. “Fully Device-Independent Quantum Key Distribution”. In: *Physical Review Letters* 113.14 (2014), Art–No.

[97] Thomas Vidick. *The Pauli Braiding Test*. Available at https://mycqstate.wordpress.com/2017/06/28/pauli-braiding/. 2017.

[98] W. T. Gowers and O. Hatami. *Inverse and stability theorems for approximate representations of finite groups*. arXiv preprint arXiv:1510.04085. 2015.

[99] Yukun Wang, Xingyao Wu, and Valerio Scarani. "All the self-testings of the singlet for two binary measurements". In: *New Journal of Physics* 18.2 (2016), p. 025021. URL: http://stacks.iop.org/1367-2630/18/i=2/a=025021.

[100] Xingyao Wu et al. "Device-independent parallel self-testing of two singlets". In: *Physical Review A* 93.6 (2016), p. 062121.

[101] Xingyao Wu et al. "Robust self-testing of the three-qubit W state". In: *Phys. Rev. A* 90.4 (2014), p. 042339.

[102] Tzyh Haur Yang and Miguel Navascués. "Robust self-testing of unknown quantum systems into any entangled two-qubit states". In: *Physical Review A* 87.5 (2013), p. 050102.

[103] Tzyh Haur Yang et al. "Robust and versatile black-box certification of quantum devices". In: *Physical review letters* 113.4 (2014), p. 040401.

Appendix A

PARALLEL SELF-TESTING VIA COPIES OF (TILTED) CHSH AND THE MAGIC SQUARE GAME

In this chapter, we show a very natural result: namely that playing n copies of the CHSH game in parallel with ideal winning probability self-tests n EPR pairs. This is covered in Section A.1 (subsection A.1.1 shows the result in the ideal case, and Subsection A.1.2 extends the analysis to the robust case). In Section A.2, we generalize the result to copies of *tilted* CHSH.

A.1 Self-Testing via n copies of CHSH in parallel

A.1.1 Ideal self-testing of n EPR pairs

Let Alice and Bob's Hilbert spaces be $\mathcal{H}_A \otimes \mathcal{H}_B$ respectively. They receive questions x, y, to which they reply with answers a, b respectively. We denote their projective measurements by $\{\Pi_{a|x}\}$ on $\mathcal{H}_A$ for Alice, and $\{\Pi_{b|y}\}$ on $\mathcal{H}_B$ for Bob. Let their joint state be $|\psi\rangle$. We take Alice and Bob's joint state to be pure for ease of exposition, but it is straightforward to check that all the proofs go through in the same way if one assumes a mixed state.

For the case of n copies of CHSH, we have $a, b, x, y \in \{0, 1, .., 2^n - 1\}$. We set:

$$x = 2^{n-1}x_1 + .. + 2x_{n-1} + x_n \qquad y = 2^{n-1}y_1 + .. + 2y_{n-1} + y_n$$
$$a = 2^{n-1}a_1 + .. + 2a_{n-1} + a_n \qquad b = 2^{n-1}b_1 + .. + 2b_{n-1} + b_n$$

with the $a_i, b_i, x_i, y_i \in \{0, 1\}$. The idea is that we are splitting the inputs and outputs as if they were received from n different CHSH tests.

In what follows, for a $\mathbf{w} = (w_1, w_2, .., w_n) \in \{0, 1\}^n$, we will denote $w = 2^{n-1}w_1 + .. + 2w_{n-1} + w_n$. Next, generalising the setup of Wu et al. [100] (in a similar fashion to what is also done by McKague in [61]) we introduce the operators

$$Z_i^{(k)} = \sum_{\mathbf{a}=(a_1,..,a_{i-1},0,a_{i+1},..,a_n)} \Pi^A_{a|x} - \sum_{\mathbf{a}=(a_1,..,a_{i-1},1,a_{i+1},..,a_n)} \Pi^A_{a|x},$$

where x is the kth smallest element of the set $\{x : \mathbf{x} = (x_1, .., x_{i-1}, 0, x_{i+1}, .., x_n)\}$, and

$$X_i^{(k)} = \sum_{\mathbf{a}=(a_1,..,a_{i-1},0,a_{i+1},..,a_n)} \Pi^A_{a|x} - \sum_{\mathbf{a}=(a_1,..,a_{i-1},1,a_{i+1},..,a_n)} \Pi^A_{a|x},$$

where x is the kth smallest element of $\{x : \mathbf{x} = (x_1, .., x_{i-1}, 1, x_{i+1}, .., x_n)\}$.
In the above, $i \in \{1, .., n\}$, and $k \in \{1, .., 2^{n-1}\}$. Here, $Z_i^{(k)}$ is the operator that Alice measures to

get her ith output bit when her ith input bit (i.e. question) is 0, and the other $n-1$ input bits are such that the overall question x is the kth smallest element of the set $\{x : \mathbf{x} = (x_1, .., x_{i-1}, 0, x_{i+1}, .., x_n)\}$ (this is just a convenient-to-state choice of ordering of questions, but there is no other particular reason for choosing this). There are 2^{n-1} possible choices for the remaining $n-1$ input bits once the ith one is fixed to be zero, and that is why k ranges from 1 to 2^{n-1}. Similarly, $X_i^{(k)}$ is the operator that Alice measures to get the ith output bit when her ith input bit 1 (instead of zero), and the index k has a meaning analogous to that for $Z_i^{(k)}$.

Now for $i = 1, .., n$ we define

$$V_i' = \frac{1}{2^{n-1}} \sum_{k=1}^{2^{n-1}} Z_i^{(k)}, \qquad W_i' = \frac{1}{2^{n-1}} \sum_{k=1}^{2^{n-1}} X_i^{(k)}.$$

Intuitively, one can think of V_i' as the operator that Alice measures to obtain her ith output bit when her ith input bit is 0 and she forgets about the other input bits, but assumes that they are uniformly distributed. W_i' is similarly defined with the difference that the ith input bit is 1.
Construct V_i' and W_i' analogously for Bob, but let the subscript i run from $n+1$ to $2n$ (we avoid defining the X_i's and Z_i's on Bob's side just yet, as we'll use these symbols differently in a moment). Notice, now, that the condition of Alice and Bob having optimal CHSH correlations in the ith game can be written as:

$$\langle\psi| \left[V_i(V_{n+i}' + W_{n+i}') + W_i(V_{n+i}' - W_{n+i}') \right] |\psi\rangle = 2\sqrt{2}.$$

Now, we can state our first parallel self-test.

Theorem 28. *Consider the setup (and the notation) described in this section, with Alice and Bob each receiving n-bit questions and producing n-bit answers, and suppose that each of the n pairs of Alice and Bob's answers has optimal CHSH correlations, i.e. for $i = 1, ..n$*

$$\langle\psi| \left[V_i(V_{n+i}' + W_{n+i}') + W_i(V_{n+i}' - W_{n+i}') \right] |\psi\rangle = 2\sqrt{2}.$$

Then there exist reflections $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$ and a local unitary $U = U_A \otimes U_B$, where $U_D \in \mathcal{L}(\mathcal{H}_D \otimes (\mathbb{C}^2)^{\otimes n}_{D^{(1)}..D^{(n)}})$ for D either A or B, and a state $|extra\rangle_{AB}$ such that

$$U(|\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) = |extra\rangle_{AB} \left|\Phi^+\right\rangle^{\otimes n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}$$
$$U(M_D^{(i)} |\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) = |extra\rangle_{AB} (\sigma^m_{D^{(i)}} \left|\Phi^+\right\rangle^{\otimes n})_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}},$$

where $(M, m) \in \{(X, x), (Z, z)\}$ and $\sigma^x_{D^{(i)}}$ and $\sigma^z_{D^{(i)}}$ are Pauli operators acting on qubit subsystem $D^{(i)}$.

In the rest of this subsection, we will be proving Theorem 28.
Now, for each of the n subtests, the optimal CHSH correlations give, for $i = 1, .., n$:

$$\frac{1}{2^{n-1}} \langle\psi| \Big[\sum_{k=1}^{2^{n-1}} Z_i^{(k)} (V'_{n+i} + W'_{n+i}) + \sum_{k=1}^{2^{n-1}} X_i^{(k)} (V'_{n+i} - W'_{n+i}) \Big] |\psi\rangle = 2\sqrt{2},$$

where we have only substituted in the definition of V_i and W_i on Alice's subsystem.
We also have $n \cdot 2^{n-1}$ separate CHSH inequalities (one for each pair (i,k)):

$$\langle\psi| \big[Z_i^{(k)} (V'_{n+i} + W'_{n+i}) + X_i^{(k)} (V'_{n+i} - W'_{n+i}) \big] |\psi\rangle \leq 2\sqrt{2}.$$

It's easy to see that since equality holds in (A.1.1), equality must also hold in all of the above $n \cdot 2^{n-1}$ separate CHSH correlations. This will be exploited shortly.
First, for $i = 1, .., n$, let

$$Z'_{n+i} := (V'_{n+i} + W'_{n+i} + \mathbb{1}_{\mathrm{Ker}(V'_{n+i} + W'_{n+i})}) |V'_{n+i} + W'_{n+i} + \mathbb{1}_{\mathrm{Ker}(V'_{n+i} + W'_{n+i})}|^{-1},$$

and

$$X'_{n+i} := (V'_{n+i} - W'_{n+i} + \mathbb{1}_{\mathrm{Ker}(V'_{n+i} - W'_{n+i})}) |V'_{n+i} - W'_{n+i} + \mathbb{1}_{\mathrm{Ker}(V'_{n+i} - W'_{n+i})}|^{-1}.$$

This is the same unitarization step that we discussed at the end of Section 3.3.

Now, we state a generalization of the swap isometry (Theorem 3 from Section 3.3) to n sets of observables and n singlets. The extra condition we require is that operators on the same side, but corresponding to different indexes i and j, commute. Actually, and this is a crucial point for what we will be able to derive in our analysis in the next sections, we only require that they commute on $|\psi\rangle$.

Proposition 8. *Let $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state. Suppose there are reflections $\{X_A^{(i)}, Z_A^{(i)}; X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$ (acting on subsystems A and B as indicated by the subscripts), such that $\forall i, j (i \neq j)$ $M_A^{(i)} N_A^{(j)} |\psi\rangle = N_A^{(j)} M_A^{(i)} |\psi\rangle$ where $M, N \in \{X, Z\}$, and similarly for subsystem B. Suppose, moreover, that for all i the following holds:*

$$\begin{aligned} Z_A^{(i)} |\psi\rangle &= Z_B^{(i)} |\psi\rangle \\ X_A^{(i)} |\psi\rangle &= X_B^{(i)} |\psi\rangle \\ Z_A^{(i)} X_A^{(i)} |\psi\rangle &= -X_A^{(i)} Z_A^{(i)} |\psi\rangle \\ Z_B^{(i)} X_B^{(i)} |\psi\rangle &= -X_B^{(i)} Z_B^{(i)} |\psi\rangle \ . \end{aligned}$$

Then there exist a local unitary $U = U_A \otimes U_B$, $U_D \in \mathcal{L}(\mathcal{H}_D \otimes (\mathbb{C}^2)^{\otimes n}_{D^{(1)}..D^{(n)}})$ for D either A or B, and a state $|extra\rangle_{AB}$ such that

$$U(|\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) = |extra\rangle_{AB} \left|\Phi^+\right\rangle^{\otimes n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}$$
$$U(M_{D^{(i)}} |\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) = |extra\rangle_{AB} (\sigma^m_{D^{(i)}} \left|\Phi^+\right\rangle^{\otimes n})_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}$$

for $(M,m) \in \{(X,x),(Z,z)\}$, where $\sigma^m_{D^{(i)}}$ is a Pauli operator on qubit subsystem $D^{(i)}$ and an identity is implied on the other subsystems.

Proof: We include a proof of this proposition in the Appendix. Note that this is an ideal case result (meaning that the operator relations required in the hypothesis are exact). For our robust result, we make use of a robust version of this proposition, which follows almost directly from results in [16].

Next, we appeal to the following Lemma from [62], which is just a specialization of Lemma 3 from Chapter 3.

Lemma 49. *([62]) Let $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state. Suppose the reflections Z'_A, X'_A, V'_B, W'_B satisfy*

$$\langle\psi|Z'_A(V'_B + W'_B) + X'_A(V'_B - W'_B)|\psi\rangle = 2\sqrt{2}\,.$$

Then, defining $Z'_B = (V'_B + W'_B + \mathbb{1}_{\mathrm{Ker}(V'_B+W'_B)})|V'_B + W'_B + \mathbb{1}_{\mathrm{Ker}(V'_B+W'_B)}|^{-1}$ and $X'_B = V'_B - W'_B + \mathbb{1}_{\mathrm{Ker}(V'_B-W'_B)})|V'_B - W'_B + \mathbb{1}_{\mathrm{Ker}(V'_B-W'_B)}|^{-1}$, we have

$$Z'_A |\psi\rangle = Z'_B |\psi\rangle$$
$$X'_A |\psi\rangle = X'_B |\psi\rangle$$
$$Z'_A X'_A |\psi\rangle = -X'_A Z'_A |\psi\rangle$$
$$Z'_B X'_B |\psi\rangle = -X'_B Z'_B |\psi\rangle\ .$$

Applying this Lemma n times for $i = 1,..,n$ with $Z^{(k)}_i, X^{(k)}_i, V'_{n+i}$ and W'_{n+i}, gives

$$Z^{(k)}_i |\psi\rangle = Z'_{n+i} |\psi\rangle$$
$$X^{(k)}_i |\psi\rangle = X'_{n+i} |\psi\rangle$$
$$Z^{(k)}_i X^{(k)}_i |\psi\rangle = -X^{(k)}_i Z^{(k)}_i |\psi\rangle$$
$$Z'_{n+i} X'_{n+i} |\psi\rangle = -X'_{n+i} Z'_{n+i} |\psi\rangle\ ,$$

where the first three hold for $k = 1,..,2^{n-1}$.

We will use the above Lemma to prove some commutation relations (on $|\psi\rangle$) between operators corresponding to different subscripts. This will allows us to exploit Proposition 8, stated earlier. Recall, also, that we already have commutation between the operators indexed with subscripts up to n and those indexed from $n+1$ to $2n$, since the former act on Alice's side and the latter on Bob's side.

Consider subscripts i, j, $(i \neq j)$. Then notice, for example, that $Z_i^{(0)}$ commutes with $Z_j^{(0)}$ (this is actual commutation, not just on $|\psi\rangle$), because, by construction, both operators are sums of the same set of orthogonal projections (the ones corresponding to question x = 0), appearing possibly with a different sign. In fact, there are 2^{n-2} pairs of superscripts $(\bar{k}, \bar{l})$ such that $[Z_i^{(\bar{k})}, Z_j^{(\bar{l})}] = 0$. Consider one such pair. Then,

$$\begin{aligned}
&\Rightarrow Z_i^{(\bar{k})} Z_j^{(\bar{l})} |\psi\rangle = Z_j^{(\bar{l})} Z_i^{(\bar{k})} |\psi\rangle \\
&\Rightarrow Z_i^{(\bar{k})} Z'_{n+j} |\psi\rangle = Z_j^{(\bar{l})} Z'_{n+i} |\psi\rangle && \text{by Eq. (A.1.1)} \\
&\Rightarrow Z'_{n+j} Z_i^{(\bar{k})} |\psi\rangle = Z'_{n+i} Z_j^{(\bar{l})} |\psi\rangle \\
&\Rightarrow Z'_{n+j} Z'_{n+i} |\psi\rangle = Z'_{n+i} Z'_{n+j} |\psi\rangle && \text{by Eq. (A.1.1)} \qquad \text{(A.1)}
\end{aligned}$$

And this holds for all $i, j \in \{1, .., n\}$. But it's easy to see that this then implies

$$Z_i^{(k)} Z_j^{(l)} |\psi\rangle = Z_j^{(l)} Z_i^{(k)} |\psi\rangle \quad \forall k, l \in \{1, .., 2^{n-1}\}\,. \qquad \text{(A.2)}$$

Similary, we also get, for all $i, j \in \{1, .., n\}$,

$$X'_{n+j} X'_{n+i} |\psi\rangle = X'_{n+i} X'_{n+j} |\psi\rangle \qquad \text{(A.3)}$$

$$\Rightarrow X_i^{(k)} X_j^{(l)} |\psi\rangle = X_j^{(l)} X_i^{(k)} |\psi\rangle \quad \forall k, l \in \{1, .., 2^{n-1}\} \qquad \text{(A.4)}$$

and

$$X'_{n+j} Z'_{n+i} |\psi\rangle = Z'_{n+i} X'_{n+j} |\psi\rangle \qquad \text{(A.5)}$$

$$\Rightarrow Z_i^{(k)} X_j^{(l)} |\psi\rangle = X_j^{(l)} Z_i^{(k)} |\psi\rangle \quad \forall k, l \in \{1, .., 2^{n-1}\}\,. \qquad \text{(A.6)}$$

We have all we need in order to apply Proposition 8. As our testing measurement operators we choose

$$\{X_i^{(1)}, Z_i^{(1)}; X'_{n+i}, Z'_{n+i}\} \quad \text{for } i = 1, .., n\,.$$

Notice that there is no particular reason for choosing superscript 1, and we could replace it with any other $k \in \{1, .., 2^{n-1}\}$. Now, for each i, the conditions of Proposition 8 are met:

$$\begin{aligned} Z_i^{(1)} |\psi\rangle &= Z'_{n+i} |\psi\rangle \\ X_i^{(1)} |\psi\rangle &= X'_{n+i} |\psi\rangle \\ Z_i^{(1)} X_i^{(1)} |\psi\rangle &= -X_i^{(1)} Z_i^{(1)} |\psi\rangle \\ Z'_{n+i} X'_{n+i} |\psi\rangle &= -X'_{n+i} Z'_{n+i} |\psi\rangle \ . \end{aligned}$$

Moreover, for each i, j $(i \neq j)$, we have the commutation relations (on $|\psi\rangle$) required by Proposition 8:

$$\begin{aligned} Z_i^{(1)} Z_j^{(1)} |\psi\rangle &= Z_j^{(1)} Z_i^{(1)} |\psi\rangle && \text{by Eq. (A.2)} \\ X_i^{(1)} X_j^{(1)} |\psi\rangle &= X_j^{(1)} X_i^{(1)} |\psi\rangle && \text{by Eq. (A.4)} \\ Z_i^{(1)} X_j^{(1)} |\psi\rangle &= X_j^{(1)} Z_i^{(1)} |\psi\rangle && \text{by Eq. (A.6)} \end{aligned}$$

and

$$\begin{aligned} Z'_{n+i} Z'_{n+j} |\psi\rangle &= Z'_{n+j} Z'_{n+i} |\psi\rangle && \text{by Eq. (A.1)} \\ X'_{n+i} X'_{n+j} |\psi\rangle &= X'_{n+j} X'_{n+i} |\psi\rangle && \text{by Eq. (A.3)} \\ Z'_{n+i} X'_{n+j} |\psi\rangle &= X'_{n+j} Z'_{n+i} |\psi\rangle && \text{by Eq. (A.5)} . \end{aligned}$$

So we can apply Proposition 8 to deduce that there exists a local unitary $U = U_A \otimes U_B$ and a state $|extra\rangle_{AB}$ such that

$$\begin{aligned} U(|\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) &= |extra\rangle_{AB} \left|\Phi^+\right\rangle^{\otimes n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}} \\ \Phi(M_{D^{(i)}} |\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) &= |extra\rangle_{AB} (\sigma^m_{D^{(i)}} \left|\Phi^+\right\rangle^{\otimes n})_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}} \end{aligned} \quad (A.7)$$

for $M \in \{X, Z\}$, where $\sigma^m_{D^{(i)}}$ is a Pauli operator on qubit subsystem $D^{(i)}$. Thus, we have proved Theorem 28.

A.1.2 Robust self-testing of n EPR pairs

In this subsection, we make the self-testing result of the previous subsection robust. We show that if Alice and Bob's correlation is close-to-optimal in each of the n copies of the CHSH game, then the state that they share is close to n EPR pairs.

Just as we constructed operators satisfying the conditions of Proposition 8 exactly, in the case that Alice and Bob's correlations are perfect in each of the n copies of the CHSH game, we will

show, next, how to construct operators that are close to satisfying those conditions when Alice and Bob exhibit close-to-optimal correlations. We will find such operators by looking (more carefully) amongst the ones we constructed earlier. We will then call on a robust version of Proposition 8, namely Theorem 30, to deduce the existence of the desired isometry.

Here, we will assume without loss of generality that Alice's and Bob's spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are of even dimension, and that their observables are balanced (meaning that the $+1$ and -1 eigenspaces have equal dimension). This assumption is required in the proof, and notice that it can always be satisfied by taking the direct sum with another space of appropriate dimension on which $|\psi\rangle$ has no mass, and extending the original operators via a direct sum with an appropriate reflection.

We state, for completeness and clarity, the robust version of the self-test of Theorem 28 that we will prove.

Theorem 29. *Consider the same setup (and the notation) of Theorem 28, with Alice and Bob each receiving n-bit questions and producing n-bit answers, and suppose that each of the n pairs of Alice and Bob's answers has CHSH correlations that are ϵ-close to optimal, i.e. for $i = 1,..n$*

$$\langle\psi|\left[V_i(V'_{n+i} + W'_{n+i}) + W_i(V'_{n+i} - W'_{n+i})\right]|\psi\rangle \geq 2\sqrt{2} - \epsilon\,. \tag{A.8}$$

Then there exist reflections $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$, a local unitary $U = U_A \otimes U_B$ where $U_D : \mathcal{H}_D \otimes (\mathbb{C}^2)_{D'}^{\otimes 2n} \to (\mathbb{C}^2)_D^{\otimes n} \otimes \hat{\mathcal{H}}_D$ for D either A or B, and a state $|extra\rangle \in \hat{\mathcal{H}}_A \otimes \hat{\mathcal{H}}_B$ such that, letting $|\psi'\rangle = |\psi\rangle \otimes |\Phi^+\rangle_{A'}^{\otimes n} \otimes |\Phi^+\rangle_{B'}^{\otimes n} \in \mathcal{H}_A \otimes (\mathbb{C}^2)_{A'}^{\otimes 2n} \otimes \mathcal{H}_B \otimes (\mathbb{C}^2)_{B'}^{\otimes 2n}$, we have that $\forall i$

$$\begin{aligned}
\|U|\psi'\rangle - |\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle\| &= O(n^{\frac{3}{2}}\sqrt{\epsilon}) \\
\|UX_D^{(i)}|\psi'\rangle - \sigma^x_{D^{(i)}}|\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle\| &= O(n^{\frac{3}{2}}\sqrt{\epsilon}) \\
\|UZ_D^{(i)}|\psi'\rangle - \sigma^z_{D^{(i)}}|\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle\| &= O(n^{\frac{3}{2}}\sqrt{\epsilon})\,,
\end{aligned}$$

where $D^{(i)}$ is the ith qubit subsystem of $(\mathbb{C}^2)_D^{\otimes n}$, and $\sigma^x_{D^{(i)}}$ and $\sigma^z_{D^{(i)}}$ are Pauli operators acting on subsystem $D^{(i)}$.

Note that here the local isometry adds, as ancillae, n EPR pairs to Alice's subsystem and n to Bob's (these EPR pairs are not shared between the two provers, but each prover has n pairs separately), while in Theorem 28, instead, the isometry added simply a product of zeros. In the remainder of this subsection, we will prove Theorem 29.

Let S denote the correlation value of a CHSH game corresponding to a certain quantum strategy. Recall that $-2\sqrt{2} \leq S \leq 2\sqrt{2}$ and that $S = 4[2Pr[\text{Win}] - 1]$, where $Pr[\text{Win}]$ is the winning probability of said strategy.

Let S_i denote the correlation value of the ith CHSH game, which is given by the LHS of equation (A.8). So, with $S_i^{(k)}$ given by the LHS of equation (A.1.1), we have $S_i = \frac{1}{2^{n-1}} \sum_{k=1}^{2^{n-1}} S_i^{(k)}$, and also $Pr[\text{Win game } i] = \frac{1}{2^{n-1}} \sum_{k=1}^{2^{n-1}} Pr[\text{Win game } i|k]$.

Now, by hypothesis we have that $S_i \geq 2\sqrt{2} - \epsilon$ for $i = 1, .., n$, i.e. for each of the n games Alice and Bob win with probability $Pr[\text{Win game } i] \geq \frac{1}{2}(\frac{\sqrt{2}}{2} + 1) - \frac{\epsilon}{8} := p_* - \frac{\epsilon}{8}$, where p_* is the ideal winning probability for CHSH.

Claim: For each i, there are at most $2^{n-3} - 1$ values of k s.t. $Pr[\text{Win game } i|k] < p_* - \frac{5}{8}\epsilon$

Proof: Suppose for a contradiction that there are at least 2^{n-3} values of k s.t. $Pr[\text{Win game } i|k] < p_* - \frac{5}{8}\epsilon$. Then

$$\begin{aligned} Pr[\text{Win game } i] &\leq \frac{1}{2^{n-1}}[(2^{n-1} - 2^{n-3})p_* + 2^{n-3}(p_* - \frac{5}{8}\epsilon)] \\ &= p_* - \frac{5}{4}\frac{\epsilon}{8} < p_* - \frac{\epsilon}{8} \end{aligned}$$

which is a contradiction.

Hence, for each i, there are at least $2^{n-2} + 2^{n-3} + 1$ values of k s.t. $Pr[\text{Win game } i|k] \geq p_* - \frac{5}{8}\epsilon \Rightarrow S_i^{(k)} \geq 8p_* - 5\epsilon - 4 = 2\sqrt{2} - 5\epsilon$.

For each i denote by G_i this set of "good" values of k.

Now, we call on a special case of Lemma 50, whose proof is found in [7] (we will use this Lemma again in its full generality in Section A.2).

The setup and notation is the same as in Subsection A.1.1, and again let $Z'_{n+i} = \frac{V'_{n+i} + W'_{n+i}}{|V'_{n+i} + W'_{n+i}|}$ and $X'_{n+i} = \frac{V'_{n+i} - W'_{n+i}}{|V'_{n+i} - W'_{n+i}|}$. Then, Lemma 50, with $\theta = \frac{\pi}{4}$, implies that for each $i = 1, .., n$ and for each $k \in G_i$ we have

$$\begin{aligned} \|X_i^{(k)} - X'_{n+i}|\psi\rangle\| \leq \epsilon_1 \qquad & \|Z_i^{(k)} - Z'_{n+i}|\psi\rangle\| \leq \epsilon_1 \\ \|(Z_i^{(k)}X_i^{(k)} + X_i^{(k)}Z_i^{(k)})|\psi\rangle\| \leq \epsilon_1 \qquad & \|(Z'_{n+i}X'_{n+i} + X'_{n+i}Z'_{n+i})|\psi\rangle\| \leq \epsilon_1, \end{aligned}$$

where $\epsilon_1 = O(\sqrt{\epsilon})$.

Next, consider i, j in $\{1, .., n\}$ with $(i \neq j)$. Just as we mentioned in the analysis of the ideal case, there are 2^{n-2} pairs of superscripts $(\bar{k}, \bar{l})$ such that $[Z_i^{(\bar{k})}, Z_j^{(\bar{l})}] = 0$, (in each pair the two superscripts correspond to the same overall questions, so for any two different pairs $(\bar{k}, \bar{l})$ and $(\bar{\bar{k}}, \bar{\bar{l}})$ it is also the case that $\bar{k} \neq \bar{\bar{k}}$ and $\bar{l} \neq \bar{\bar{l}}$). It is easy to see, then, that since there are at most $2^{n-3} - 1$ values of $k \in \{1, .., 2^{n-1}\}$ such that $k \notin G_i$ and at most $2^{n-3} - 1$ values of $l \in \{1, .., 2^{n-1}\}$ such that $l \notin G_j$, there must be at least one pair $(\bar{k}, \bar{l})$ such that $[Z_i^{(\bar{k})}, Z_j^{(\bar{l})}] = 0$ and such that both $\bar{k} \in G_i$ and $\bar{l} \in G_j$. So, $Z_i^{(\bar{k})}Z_j^{(\bar{l})}|\psi\rangle = Z_j^{(\bar{l})}Z_i^{(\bar{k})}|\psi\rangle$ and using equation (A.1.2) and triangle inequalities

we have:

$$\begin{aligned} &\|(Z_i^{(\bar{k})} Z'_{n+j} - Z_j^{(\bar{l})} Z'_{n+i}) \,|\psi\rangle\| \leq 2\epsilon_1 \\ &\|(Z'_{n+j} Z'_{n+i} - Z'_{n+i} Z'_{n+j}) \,|\psi\rangle\| \leq 4\epsilon_1 \\ \Rightarrow &\|(Z_i^{(k)} Z_j^{(l)} - Z_j^{(l)} Z_i^{(k)} \,|\psi\rangle\| \leq 8\epsilon_1 \quad \text{for all } k \in G_i, l \in G_j \,. \end{aligned}$$

Similarly we also find

$$\begin{aligned} &\|(X'_{n+j} X'_{n+i} - X'_{n+i} X'_{n+j}) \,|\psi\rangle\| \leq 4\epsilon_1 \\ \Rightarrow &\|(X_i^{(k)} X_j^{(l)} - X_j^{(l)} X_i^{(k)} \,|\psi\rangle\| \leq 8\epsilon_1 \quad \text{for all } k \in G_i, l \in G_j \end{aligned}$$

and

$$\begin{aligned} &\|(X'_{n+j} Z'_{n+i} - Z'_{n+i} X'_{n+j}) \,|\psi\rangle\| \leq 4\epsilon_1 \\ \Rightarrow &\|(Z_i^{(k)} X_j^{(l)} - X_j^{(l)} Z_i^{(k)} \,|\psi\rangle\| \leq 8\epsilon_1 \quad \text{for all } k \in G_i, l \in G_j \,. \end{aligned}$$

Now, we state a robust version of Proposition 8, which follows almost directly from results in [16], upon straightening out small details. The results from [16] are stated precisely in the Appendix (Theorems 34 and 35).

Theorem 30. *Let $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state, where $\mathcal{H}_A$ and $\mathcal{H}_B$ have even dimension. Suppose there are balanced reflections $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$ such that, for D either A or B and for all $i \neq j$, they satisfy*

$$\begin{aligned} \|M_A^{(i)} \,|\psi\rangle - M_B^{(i)} \,|\psi\rangle\| &\leq \epsilon \\ \|\{X_D^{(i)}, Z_D^{(i)}\} \,|\psi\rangle\| &\leq \epsilon \\ \|\,[M_D^{(i)}, N_D^{(j)}] \,|\psi\rangle\| &\leq \epsilon \,, \end{aligned}$$

where $M, N \in \{X, Z\}$.
Then, letting $|\psi'\rangle = |\psi\rangle \otimes |\Phi^+\rangle_{A'}^{\otimes n} \otimes |\Phi^+\rangle_{B'}^{\otimes n} \in \mathcal{H}_A \otimes (\mathbb{C}^2)_{A'}^{\otimes 2n} \otimes \mathcal{H}_B \otimes (\mathbb{C}^2)_{B'}^{\otimes 2n}$, there exist a local unitary $U = U_A \otimes U_B$ where $U_D : \mathcal{H}_D \otimes (\mathbb{C}^2)_{D'}^{\otimes 2n} \to (\mathbb{C}^2)_D^{\otimes n} \otimes \hat{\mathcal{H}}_D$ and a state $|extra\rangle \in \hat{\mathcal{H}}_A \otimes \hat{\mathcal{H}}_B$ such that $\forall i$

$$\begin{aligned} \|U \,|\psi'\rangle - |\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle\| &= O(n^{\frac{3}{2}}\epsilon) \\ \|UX_D^{(i)} \,|\psi'\rangle - \sigma_{D^{(i)}}^x \,|\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle\| &= O(n^{\frac{3}{2}}\epsilon) \\ \|UZ_D^{(i)} \,|\psi'\rangle - \sigma_{D^{(i)}}^z \,|\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle\| &= O(n^{\frac{3}{2}}\epsilon) \,, \end{aligned}$$

where $D^{(i)}$ is the ith qubit subsystem of $(\mathbb{C}^2)_D^{\otimes n}$, and $\sigma_{D^{(i)}}^x$ and $\sigma_{D^{(i)}}^z$ are Pauli operators acting on subsystem $D^{(i)}$.

Proof: Except for one small detail (which is dealt with in the Appendix), this Theorem follows already from results in [16]. These are stated precisely in the Appendix (as Theorems 34, 35), although we refer the reader to their source ([16]) for their proof.

We are now in the position to apply Theorem 30 to the following choice of operators. For each $i = 1, .., n$ fix a $k_i \in G_i$. The choice of operators is then $\{X_i^{(k_i)}, Z_i^{(k_i)}, X'_{n+i}, Z'_{n+i}\}$, for $i = 1, .., n$. These, as we have shown, satisfy all conditions of Theorem 30, with $O(\epsilon_1)$ bound. Now, recall that $\epsilon_1 = O(\sqrt{\epsilon})$. This implies, by Theorem 30, that there exists a local isometry, which adds n EPR pairs on each side (separately) as ancillae, sending $|\psi\rangle$ to a state that is $O(n^{\frac{3}{2}}\sqrt{\epsilon})$-close to a product of n EPR pairs shared between Alice and Bob, with the action of the constructed operators on $|\psi\rangle$ mapping to that of the appropriate Pauli operators. This completes the proof of Theorem 29.

A.2 Self-Testing via n copies of tilted CHSH

In this section, we generalize self-testing of n EPR pairs in parallel via n copies of CHSH to self-testing of n *tilted* EPR pairs via n copies of *tilted* CHSH. To aid exposition, we will treat the ideal case (subsection 31) before the robust case (subsection 32).

A.2.1 Ideal self-testing of n tilted EPR pairs

First, recall that we already know ([102], [7]) how to self-test a single pair of partially entangled qubits $|\psi_\theta\rangle := \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$. In fact, observing maximal violation of the tilted CHSH inequality, i.e.

$$\alpha A_o + A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 = \sqrt{8 + 2\beta^2}$$

self-tests the state $|\psi_\theta\rangle$, where $\sin(2\theta) = \sqrt{\frac{4-\beta^2}{4+\beta^2}}$.

We naturally extend this to the parallel setting, and ask whether observing n pairs of answers that individually maximally violate the tilted CHSH inequality for some θ_i's (possibly different) self-tests a tensor product of tilted EPR pairs with the corresponding angles θ_i, namely $\bigotimes_{i=1}^n |\psi_{\theta_i}\rangle$.

Define V'_i and W'_i for $i = 1, .., 2n$ in the same way as in Section A.1. Then, our self-testing theorem in the ideal case is the following.

Theorem 31. *Consider the setup (and the notation) of Section A.1, with Alice and Bob each receiving n-bit questions and producing n-bit answers. Suppose that there are angles θ_i, $i = 1, .., n$, such that the ith of the n pairs of Alice and Bob's answers has optimal tilted CHSH correlations with angle θ_i, i.e. for $i = 1, .., n$*

$$\langle\psi|\left[\beta_i V_i + V_i(V'_{n+i} + W'_{n+i}) + W_i(V'_{n+i} - W'_{n+i})\right]|\psi\rangle = \sqrt{8 + 2\beta_i^2}\,,$$

where $\sin(2\theta_i) = \sqrt{\frac{4-\beta_i^2}{4+\beta_i^2}}$. *Then there exist reflections* $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$ *and a local unitary* $U = U_A \otimes U_B$, *where* $U_D \in \mathcal{L}(\mathcal{H}_D \otimes (\mathbb{C}^2)^{\otimes n}_{D^{(1)}..D^{(n)}})$ *for* D *either* A *or* B, *and a state* $|extra\rangle_{AB}$ *such that*

$$U(|\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) = |extra\rangle_{AB} \, (\bigotimes_{j=1}^{n} \left|\psi_{\theta_j}\right\rangle)_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}$$

$$U(M_D^{(i)} |\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) = |extra\rangle_{AB} \left(\sigma^m_{D^{(i)}} (\bigotimes_{j=1}^{n} \left|\psi_{\theta_j}\right\rangle)_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}\right),$$

where $(M, m) \in \{(X, x), (Z, z)\}$ *and* $\sigma^x_{D^{(i)}}$ *and* $\sigma^z_{D^{(i)}}$ *are Pauli operators acting on qubit subsystem* $D^{(i)}$.

Now, by hypothesis each of the n pairs of answers maximally violates the tilted CHSH inequality for some angle θ_i. Then, recalling the definitions of $Z_i^{(k)}$ and $X_i^{(k)}$ from Section A.1, we have, for $i = 1, .., n$:

$$\frac{1}{2^{n-1}} \langle\psi| \Big[\sum_{k=1}^{2^{n-1}} \beta_i Z_i^{(k)} + \sum_{k=1}^{2^{n-1}} Z_i^{(k)} (V'_{n+i} + W'_{n+i}) + \sum_{k=1}^{2^{n-1}} X_i^{(k)} (V'_{n+i} - W'_{n+i}) \Big] |\psi\rangle = \sqrt{8 + 2\beta_i^2}\,, \tag{A.9}$$

where $\sin(2\theta_i) = \sqrt{\frac{4-\beta_i^2}{4+\beta_i^2}}$.

We also have $n \cdot 2^{n-1}$ separate tilted CHSH inequalities (one for each pair (i, k)):

$$\langle\psi| \left[\beta_i Z_i^{(k)} + Z_i^{(k)} (V'_{n+i} + W'_{n+i}) + X_i^{(k)} (V'_{n+i} - W'_{n+i})\right] |\psi\rangle \leq \sqrt{8 + 2\beta_i^2}\,. \tag{A.10}$$

But we deduce that, since equality must hold in $(A.9)$, then equality must hold in all of the above $n \cdot 2^{n-1}$ tilted CHSH inequalities. We will exploit this thanks to Lemma 3 (from Bamps and Pironio [7]), which we restate here for clarity:

Lemma 50. *([7])Let* $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ *be a bipartite state. Suppose that reflections* Z'_A, X'_A, V'_B, W'_B *satisfy*

$$\langle\psi| \, \beta Z'_A + Z'_A (V'_B + W'_B) + X'_A (V'_B - W'_B) |\psi\rangle = \sqrt{8 + 2\beta^2}\,.$$

Then, defining $Z'_B = (V'_B + W'_B + \mathbb{1}_{\mathrm{Ker}(V'_B + W'_B)}) |V'_B + W'_B + \mathbb{1}_{\mathrm{Ker}(V'_B + W'_B)}|^{-1}$ *and* $X'_B = V'_B - W'_B + \mathbb{1}_{\mathrm{Ker}(V'_B - W'_B)}) |V'_B - W'_B + \mathbb{1}_{\mathrm{Ker}(V'_B - W'_B)}|^{-1}$, *we have*

$$Z'_A |\psi\rangle = Z'_B |\psi\rangle$$
$$\sin\theta X'_A (I + Z'_B) |\psi\rangle = \cos\theta X'_B (I - Z'_A) |\psi\rangle$$
$$Z'_A X'_A |\psi\rangle = -X'_A Z'_A |\psi\rangle, \qquad Z'_B X'_B |\psi\rangle = -X'_B Z'_B |\psi\rangle\,,$$

where $\sin(2\theta) = \sqrt{\frac{4-\beta^2}{4+\beta^2}}$ *and* $\tan\mu = \sin(2\theta)$.

Now, define

$$Z'_{n+i} := (V'_{n+i} + W'_{n+i} + \mathbb{1}_{\mathrm{Ker}(V'_{n+i}+W'_{n+i})})|V'_{n+i} + W'_{n+i} + \mathbb{1}_{\mathrm{Ker}(V'_{n+i}+W'_{n+i})}|^{-1},$$

and

$$X'_{n+i} := (V'_{n+i} - W'_{n+i} + \mathbb{1}_{\mathrm{Ker}(V'_{n+i}-W'_{n+i})})|V'_{n+i} - W'_{n+i} + \mathbb{1}_{\mathrm{Ker}(V'_{n+i}-W'_{n+i})}|^{-1}.$$

Then, by Lemma 50 we have that for each $i = 1,..,,n$ and $k = 1,..,2^{n-1}$ the following two relations are satisfied:

$$Z_i^{(k)} |\psi\rangle = Z'_{n+i} |\psi\rangle \tag{A.11}$$

$$\sin\theta_i X_i^{(k)} (I + Z'_{n+i}) |\psi\rangle = \cos\theta_i X'_{n+i} (I - Z_i^{(k)}) |\psi\rangle \ . \tag{A.12}$$

We will also make use of the following further generalization of Proposition 8.

Proposition 9. *Let* $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ *be a bipartite state. Suppose there are reflections* $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$*, and angles* θ_i*,* $i = 1,..,n$*, such that the following conditions are satisfied for each* i*:*

$$Z_A^{(i)} |\psi\rangle = Z_B^{(i)} |\psi\rangle \tag{A.13}$$

$$\sin\theta_i X_A^{(i)} (I + Z_B^{(i)}) |\psi\rangle = \cos\theta_i X_B^{(i)} (I - Z_A^{(i)}) |\psi\rangle \ . \tag{A.14}$$

Suppose, in addition, that $\forall i, j (i \neq j)$ *we have* $M_A^{(i)} N_A^{(j)} |\psi\rangle = N_A^{(j)} M_A^{(i)} |\psi\rangle$ *where* $M, N \in \{X, Z\}$*, and similarly for subsystem B.*
Then, there exists a local unitary $U = U_A \otimes U_B$*, where* $U_D \in \mathcal{L}(\mathcal{H}_D \otimes (\mathbb{C}^2)^{\otimes n}_{D^{(1)}..D^{(n)}})$ *for* D *either A or B, and a state* $|extra\rangle_{AB}$ *such that*

$$U(|\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) = |extra\rangle_{AB} \left(\bigotimes_{j=1}^{n} \left|\psi_{\theta_j}\right\rangle\right)_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}$$

$$U(M_D^{(i)} |\psi\rangle_{AB} |0\rangle^{\otimes 2n}_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}) = |extra\rangle_{AB} \left(\sigma^m_{D^{(i)}} \left(\bigotimes_{j=1}^{n} \left|\psi_{\theta_j}\right\rangle\right)_{A^{(1)}B^{(1)}..A^{(n)}B^{(n)}}\right),$$

where $(M, m) \in \{(X, x), (Z, z)\}$ *and* $\sigma^x_{D^{(i)}}$ *and* $\sigma^z_{D^{(i)}}$ *are Pauli operators acting on qubit subsystem* $D^{(i)}$.

Proof: See the auxiliary results of Section A.3.

We have already argued above, that $Z_i^{(k)}$, $X_i^{(k)}$, Z'_{n+i} and X'_{n+i} as defined earlier satisfy conditions (A.13) and (A.14) for $i = 1,..n$ and $k = 1,..,2^{n-1}$.
Recall, that we already know that operators indexed with subscripts from 1 to n commute with those indexed from $n+1$ to $2n$, since they act on Alice's side and Bob's side respectively. So, it is sufficient for us to show that for each i we can make a choice of $\tilde{k}$ (possibly depending on i) such that the commutation relations of Proposition 9 are satisfied for each $i \neq j$ when we set $Z_A^{(i)} = Z_i^{(\tilde{k})}$, $X_A^{(i)} = X_i^{(\tilde{k})}$, $Z_B^{(i)} = Z'_{n+i}$ and $X_B^{(i)} = X'_{n+i}$, for $i = 1,..,n$. This is what we will show next, in a similar (although slightly more involved) fashion to the case of non-tilted CHSH in Section A.1.

First, notice, just as in Section A.1, that for each $i \neq j$ one can pick $\bar{k},\bar{l} \in \{1,..,2^{n-1}\}$ such that $[Z_i^{(\bar{k})}, Z_j^{(\bar{l})}] = 0$ (there are 2^{n-2} such pairs $\bar{k},\bar{l}$). Then

$$\begin{aligned}
&\Rightarrow Z_i^{(\bar{k})} Z_j^{(\bar{l})} |\psi\rangle = Z_j^{(\bar{l})} Z_i^{(\bar{k})} |\psi\rangle \\
&\Rightarrow Z_i^{(\bar{k})} Z'_{n+j} |\psi\rangle = Z_j^{(\bar{l})} Z'_{n+i} |\psi\rangle && \text{by Eq. (A.11)} \\
&\Rightarrow Z'_{n+j} Z_i^{(\bar{k})} |\psi\rangle = Z'_{n+i} Z_j^{(\bar{l})} |\psi\rangle \\
&\Rightarrow Z'_{n+j} Z'_{n+i} |\psi\rangle = Z'_{n+i} Z'_{n+j} |\psi\rangle && \text{by Eq. (A.11)}. \qquad \text{(A.15)}
\end{aligned}$$

But then equation (A.15) implies, by condition (A.11), that

$$Z_i^{(k)} Z_j^{(l)} |\psi\rangle = Z_j^{(l)} Z_i^{(k)} |\psi\rangle \quad \forall k,l \in \{1,..,2^{n-1}\}$$

and this holds for all $i \neq j$.

The same exact trick, as one can easily see, doesn't quite work for pairs X,Z and X,X and things are slightly trickier. First, we will show that, $\forall i \neq j$ and $\forall k,l$,

$$X_i^{(k)}(I - Z_i^{(k)}) Z_j^{(l)} |\psi\rangle = Z_j^{(l)} X_i^{(k)}(I - Z_i^{(k)}) |\psi\rangle \qquad \text{(A.16)}$$

$$X_i^{(k)}(I + Z_i^{(k)}) Z_j^{(l)} |\psi\rangle = Z_j^{(l)} X_i^{(k)}(I + Z_i^{(k)}) |\psi\rangle \ . \qquad \text{(A.17)}$$

For any $i \neq j$ one can pick $\bar{k},\bar{l} \in \{1,..,2^{n-1}\}$ such that $[X_i^{(\bar{k})}, Z_j^{(\bar{l})}] = 0$. Then

$$\Rightarrow X_i^{(\bar{k})}(I - Z_i^{(\bar{k})}) Z_j^{(\bar{l})} |\psi\rangle = Z_j^{(\bar{l})} X_i^{(\bar{k})}(I - Z_i^{(\bar{k})}) |\psi\rangle \qquad \text{(A.18)}$$

since we have already shown that $Z_i^{(k)} Z_j^{(l)} |\psi\rangle = Z_j^{(l)} Z_i^{(k)} |\psi\rangle$ for all k,l. Then, notice that by multiplying both sides of (A.12) by $X_i^{(k)} X'_{n+i}$ we also have

$$\sin\theta_i X'_{n+i}(I + Z'_{n+i}) |\psi\rangle = \cos\theta_i X_i^{(k)}(I - Z_i^{(k)}) |\psi\rangle \ . \qquad \text{(A.19)}$$

Hence, using (A.19) and (A.11) in (A.18), we get

$$\begin{aligned} &\tan\theta_i Z'_{n+j}X'_{n+i}(I+Z'_{n+i})\,|\psi\rangle = \tan\theta_i X'_{n+i}(I+Z'_{n+i})Z'_{n+j}\,|\psi\rangle \qquad (A.20)\\ \Rightarrow &X_i^{(k)}(I-Z_i^{(k)})Z_j^{(l)}\,|\psi\rangle = Z_j^{(l)}X_i^{(k)}(I-Z_i^{(k)})\,|\psi\rangle \text{ again by (A.19) and (A.11),} \end{aligned}$$

where the last line holds for all k,l.

Finally, if we start from

$$X_i^{(\bar{k})}(I+Z_i^{(\bar{k})})Z_j^{(\bar{l})}\,|\psi\rangle = Z_j^{(\bar{l})}X_i^{(\bar{k})}(I+Z_i^{(\bar{k})})\,|\psi\rangle\ ,$$

where we have only changed a plus to a minus from (A.18), then we similarly obtain

$$\cot\theta_i Z'_{n+j}X'_{n+i}(I-Z'_{n+i})\,|\psi\rangle = \cot\theta_i X'_{n+i}(I-Z'_{n+i})Z'_{n+j}\,|\psi\rangle\ , \qquad (A.21)$$

and the latter implies (A.17).
Relations (A.16) and (A.17) also hold for subsystem B, as we have obtained along the way in (A.20) and (A.21).
Hence now, summing up (A.16) and (A.17) gives precisely

$$X_i^{(k)}Z_j^{(l)}\,|\psi\rangle = Z_j^{(l)}X_i^{(k)}\,|\psi\rangle \qquad \forall k,l$$

and similarly we obtain

$$Z'_{n+j}X'_{n+i}\,|\psi\rangle = X'_{n+i}Z'_{n+j}\,.\,|\psi\rangle$$

We are left to obtain the X,X commutation. For any $i\neq j$ one can pick $\bar{k}$,$\bar{l}\in\{1,..,2^{n-1}\}$ such that $[X_i^{(\bar{k})},X_j^{(\bar{l})}]=0$. Then $X_i^{(\bar{k})}X_j^{(\bar{l})}\,|\psi\rangle = X_j^{(\bar{l})}X_i^{(\bar{k})}\,|\psi\rangle$.
Now, apply $(I+Z'_{n+i})(I+Z'_{n+j})$ to both sides, to obtain

$$X_i^{(\bar{k})}(I+Z'_{n+i})X_j^{(\bar{l})}(I+Z'_{n+j})\,|\psi\rangle = X_j^{(\bar{l})}(I+Z'_{n+j})X_i^{(\bar{k})}(I+Z'_{n+i})\,|\psi\rangle\ ,$$

where we have used commutativity of Z'_{n+i} and Z'_{n+j} on $|\psi\rangle$.

$$\begin{aligned} &\Rightarrow X_i^{(\bar{k})}(I+Z'_{n+i})[\cot\theta_j X'_{n+j}(I-Z'_{n+j})]\,|\psi\rangle = X_j^{(\bar{l})}(I+Z'_{n+j})[\cot\theta_i X'_{n+i}(I-Z'_{n+i})]\,|\psi\rangle\\ &\Rightarrow\quad [\cot\theta_j X'_{n+j}(I-Z'_{n+j})][\cot\theta_i X'_{n+i}(I-Z'_{n+i})]\,|\psi\rangle\\ &\qquad = [\cot\theta_i X'_{n+i}(I-Z'_{n+i})][\cot\theta_j X'_{n+j}(I-Z'_{n+j})]\,|\psi\rangle\\ &\Rightarrow \cancel{\cot\theta_i\cot\theta_j}\,[X'_{n+j}X'_{n+i}\,|\psi\rangle - X'_{n+j}Z'_{n+j}X'_{n+i}\,|\psi\rangle - X'_{n+j}X'_{n+i}Z'_{n+i}\,|\psi\rangle + X'_{n+j}Z'_{n+j}X'_{n+i}Z'_{n+i}\,|\psi\rangle]\\ &\qquad = \cancel{\cot\theta_i\cot\theta_j}\,[i\leftrightarrow j]\,, \qquad (A.22) \end{aligned}$$

where to get the second line we used Z,Z and X,Z commutativity and a simple trick from the auxiliary results (Section A.3) which allows to commute operators when they are not directly in front of $|\psi\rangle$.
Now, if we start from $X_i^{(\bar{k})}X_j^{(\bar{l})}|\psi\rangle = X_j^{(\bar{l})}X_i^{(\bar{k})}|\psi\rangle$ by applying $(I - Z'_{n+i})(I - Z'_{n+j})$ to both sides instead, then we obtain, in a similar fashion,

$$\cancel{\tan\theta_i \tan\theta_j}\,[X'_{n+j}X'_{n+i}|\psi\rangle + X'_{n+j}Z'_{n+j}X'_{n+i}|\psi\rangle + X'_{n+j}X'_{n+i}Z'_{n+i}|\psi\rangle + X'_{n+j}Z'_{n+j}X'_{n+i}Z'_{n+i}|\psi\rangle]$$
$$= \cancel{\tan\theta_i \tan\theta_j}\,[i \leftrightarrow j]\,. \tag{A.23}$$

And now,

$$\begin{aligned}\text{(A.22)} + \text{(A.23)} \Rightarrow & X'_{n+j}X'_{n+i}|\psi\rangle + X'_{n+j}Z'_{n+j}X'_{n+i}Z'_{n+i}|\psi\rangle \\ & = X'_{n+i}X'_{n+j}|\psi\rangle + X'_{n+i}Z'_{n+i}X'_{n+j}Z'_{n+j}|\psi\rangle \end{aligned}\tag{A.24}$$

Now, similarly starting by applying $(I + Z'_{n+i})(I - Z'_{n+j})$ to $X_i^{(\bar{k})}X_j^{(\bar{l})}|\psi\rangle = X_j^{(\bar{l})}X_i^{(\bar{k})}|\psi\rangle$, we obtain

$$\cancel{\cot\theta_i \tan\theta_j}\,[X'_{n+j}X'_{n+i}|\psi\rangle + X'_{n+j}Z'_{n+j}X'_{n+i}|\psi\rangle - X'_{n+j}X'_{n+i}Z'_{n+i}|\psi\rangle - X'_{n+j}Z'_{n+j}X'_{n+i}Z'_{n+i}|\psi\rangle]$$
$$= \cancel{\cot\theta_i \tan\theta_j}\,[X'_{n+i}X'_{n+j}|\psi\rangle - X'_{n+i}Z'_{n+i}X'_{n+j}|\psi\rangle + X'_{n+i}X'_{n+j}Z'_{n+j}|\psi\rangle - X'_{n+i}Z'_{n+i}X'_{n+j}Z'_{n+j}|\psi\rangle]\,. \tag{A.25}$$

And similarly, starting by applying $(I - Z'_{n+i})(I + Z'_{n+j})$ to $X_i^{(\bar{k})}X_j^{(\bar{l})}|\psi\rangle = X_j^{(\bar{l})}X_i^{(\bar{k})}|\psi\rangle$, we obtain

$$\cancel{\tan\theta_i \cot\theta_j}\,[X'_{n+j}X'_{n+i}|\psi\rangle - X'_{n+j}Z'_{n+j}X'_{n+i}|\psi\rangle + X'_{n+j}X'_{n+i}Z'_{n+i}|\psi\rangle - X'_{n+j}Z'_{n+j}X'_{n+i}Z'_{n+i}|\psi\rangle]$$
$$= \cancel{\tan\theta_i \cot\theta_j}\,[X'_{n+i}X'_{n+j}|\psi\rangle + X'_{n+i}Z'_{n+i}X'_{n+j}|\psi\rangle - X'_{n+i}X'_{n+j}Z'_{n+j}|\psi\rangle - X'_{n+i}Z'_{n+i}X'_{n+j}Z'_{n+j}|\psi\rangle]\,. \tag{A.26}$$

And so,

$$\begin{aligned}\text{(A.25)} + \text{(A.26)} \Rightarrow & X'_{n+j}X'_{n+i}|\psi\rangle - X'_{n+j}Z'_{n+j}X'_{n+i}Z'_{n+i}|\psi\rangle \\ & = X'_{n+i}X'_{n+j}|\psi\rangle - X'_{n+i}Z'_{n+i}X'_{n+j}Z'_{n+j}|\psi\rangle\,. \end{aligned}\tag{A.27}$$

And finally,

$$\text{(A.24)} + \text{(A.27)} \Rightarrow X'_{n+j}X'_{n+i}|\psi\rangle = X'_{n+i}X'_{n+j}|\psi\rangle\,.$$

And from this, simply by running the same calculations swapping the roles of subsystems A and B we are able to also obtain

$$X_i^{(k)}X_j^{(l)}|\psi\rangle = X_j^{(l)}X_i^{(k)}|\psi\rangle \text{ and this holds } \forall k,l \text{ (not just } \bar{k},\bar{l}\,!)\,.$$

Thus, we have shown that the commutation conditions of Proposition 9 are satisfied for both subsystems A and B for all $i \neq j$ when we set $Z_A^{(i)} = Z_i^{(k)}$, $X_A^{(i)} = X_i^{(k)}$, $Z_B^{(i)} = Z'_{n+i}$, $X_B^{(i)} = X'_{n+i}$ and $Z_A^{(j)} = Z_j^{(l)}$, $X_A^{(j)} = X_j^{(l)}$, $Z_B^{(j)} = Z'_{n+j}$ and $X_B^{(j)} = X'_{n+j}$. And this is true for any choice of $k, l \in \{1, .., 2^{n-1}\}$.

Hence, for instance, the set of operators $\{Z_i^{(1)}, X_i^{(1)}, Z'_{n+i}, X'_{n+i}\}_{i=1,..,n}$ satisfies the hypothesis of Theorem 9, and this implies the existence of the desired isometry, completing the proof of Theorem 31.

A.2.2 Robust self-testing of n tilted EPR pairs

In a similar vein to Subsection A.1.2, we show that if the correlation of Alice and Bob is close to maximally violating n tilted CHSH inequalities for angles θ_i, $i = 1, .., n$, then the joint state of Alice and Bob must be close to a tensor product of n tilted EPR pairs with the angles θ_i.
Again, we assume without loss of generality that Alice and Bob's spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are of even dimension, and that their observables are balanced.
The precise self-testing statement is the following:

Theorem 32. *Consider the setup (and the notation) of Section A.1, with Alice and Bob each receiving n-bit questions and producing n-bit answers. Suppose that there are angles θ_i, $i = 1, .., n$, such that the ith of the n pairs of Alice and Bob's answers has ϵ-close to optimal tilted CHSH correlations with angle θ_i, i.e. for $i = 1, .., n$*

$$\langle\psi| \left[\beta_i V_i + V_i(V'_{n+i} + W'_{n+i}) + W_i(V'_{n+i} - W'_{n+i})\right] |\psi\rangle \geq \sqrt{8 + 2\beta_i^2} - \epsilon\,,$$

where $\sin(2\theta_i) = \sqrt{\frac{4-\beta_i^2}{4+\beta_i^2}}$.
Then, there exist reflections $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$, a local unitary $U = U_A \otimes U_B$ where $U_D : \mathcal{H}_D \otimes (\mathbb{C}^2)_{D'}^{\otimes 2n} \to (\mathbb{C}^2)_D^{\otimes n} \otimes \hat{\mathcal{H}}_D$ for D either A or B, and a state $|extra\rangle \in \hat{\mathcal{H}}_A \otimes \hat{\mathcal{H}}_B$ such that, letting $|\psi'\rangle = |\psi\rangle \otimes \left(\bigotimes_{i=1}^n |\psi_{\theta_i}\rangle\right)_{A'} \otimes \left(\bigotimes_{i=1}^n |\psi_{\theta_i}\rangle\right)_{B'} \in \mathcal{H}_A \otimes (\mathbb{C}^2)_{A'}^{\otimes 2n} \otimes \mathcal{H}_B \otimes (\mathbb{C}^2)_{B'}^{\otimes 2n}$ we have that $\forall i$

$$\|U|\psi'\rangle - \left(\bigotimes_{j=1}^n \left|\psi_{\theta_j}\right\rangle\right)_{AB} \otimes |extra\rangle\| = O(n^2\sqrt{\epsilon})$$

$$\|UX_D^{(i)}|\psi'\rangle - \sigma^x_{D^{(i)}}\left(\bigotimes_{j=1}^n \left|\psi_{\theta_j}\right\rangle\right)_{AB} \otimes |extra\rangle\| = O(n^2\sqrt{\epsilon})$$

$$\|UZ_D^{(i)}|\psi'\rangle - \sigma^z_{D^{(i)}}\left(\bigotimes_{j=1}^n \left|\psi_{\theta_j}\right\rangle\right)_{AB} \otimes |extra\rangle\| = O(n^2\sqrt{\epsilon})\,,$$

where $D^{(i)}$ is the ith qubit subsystem of $(\mathbb{C}^2)_D^{\otimes n}$, and $\sigma^x_{D^{(i)}}$ and $\sigma^z_{D^{(i)}}$ are Pauli operators acting on subsystem $D^{(i)}$.

In proving Theorem 32 we will naturally need robust versions of Lemmas 50 and 9. The former is from [7], given below as Lemma 51, while the latter follows almost directly from results in [16], given below as Theorem 33.

Lemma 51 ([7])**.** *Let $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state. Suppose that reflections Z'_A, X'_A, V'_B, W'_B satisfy*

$$\langle\psi|\ \beta Z'_A + Z'_A(V'_B + W'_B) + X'_A(V'_B - W'_B)|\psi\rangle \geq \sqrt{8 + 2\beta^2} - \epsilon\,.$$

Then, defining $Z''_B := \frac{V'_B + W'_B}{2\cos\mu}$ and $X''_B := \frac{V'_B - W'_B}{2\sin\mu}$, and letting $Z'_B := \frac{\tilde{Z}''_B}{|\tilde{Z}''_B|}$ and $X'_B := \frac{\tilde{X}''_B}{|\tilde{X}''_B|}$ (here $\tilde{Z}''_B$ is Z''_B with the 0 eigenvalues changed to 1, and similarly for $\tilde{X}''_B$), we have

$$\begin{aligned}
\|(Z'_A - Z'_B)\,|\psi\rangle\,\| &\leq O(\sqrt{\epsilon}) \\
\|\sin\theta X'_A(I + Z'_B)\,|\psi\rangle - \cos\theta X'_B(I - Z'_A)\,|\psi\rangle\,\| &\leq O(\sqrt{\epsilon}) \\
\|(Z'_A X'_A + X'_A Z'_A)\,|\psi\rangle\,\| \leq O(\sqrt{\epsilon}) \qquad \|(Z'_B X'_B + X'_B Z'_B)\,|\psi\rangle\,\| &\leq O(\sqrt{\epsilon})\,,
\end{aligned}$$

where $\sin(2\theta) = \sqrt{\frac{4-\beta^2}{4+\beta^2}}$ and $\tan\mu = \sin(2\theta)$.

Theorem 33. *Let $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are of even dimension. Suppose there are balanced reflections $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$ and angles θ_i, $i = 1, .., n$, such that, for D either A or B and for all $i \neq j$, they satisfy:*

$$\|Z_A^{(i)}\,|\psi\rangle - Z_B^{(i)}\,|\psi\rangle\,\| \leq \epsilon \tag{A.28}$$

$$\|\sin\theta_i X_A^{(i)}(I + Z_B^{(i)})\,|\psi\rangle - \cos\theta_i X_B^{(i)}(I - Z_A^{(i)})\,|\psi\rangle\,\| \leq \epsilon \tag{A.29}$$

$$\begin{aligned}
\|\{X_D^{(i)}, Z_D^{(i)}\}\,|\psi\rangle\,\| &\leq \epsilon \\
\|\,[M_D^{(i)}, N_D^{(j)}]\,|\psi\rangle\,\| &\leq \epsilon\,,
\end{aligned}$$

where $M, N \in \{X, Z\}$.
Then, letting $|\psi'\rangle = |\psi\rangle \otimes \left(\bigotimes_{i=1}^n |\psi_{\theta_i}\rangle\right)_{A'} \otimes \left(\bigotimes_{i=1}^n |\psi_{\theta_i}\rangle\right)_{B'} \in \mathcal{H}_A \otimes (\mathbb{C}^2)_{A'}^{\otimes 2n} \otimes \mathcal{H}_B \otimes (\mathbb{C}^2)_{B'}^{\otimes 2n}$, there exist a local unitary $U = U_A \otimes U_B$ where $U_D : \mathcal{H}_D \otimes (\mathbb{C}^2)_{D'}^{\otimes 2n} \to (\mathbb{C}^2)_D^{\otimes n} \otimes \hat{\mathcal{H}}_D$

and a state $|extra\rangle \in \hat{\mathcal{H}}_A \otimes \hat{\mathcal{H}}_B$ *such that* $\forall i$

$$\begin{aligned}
\|U|\psi'\rangle - (\bigotimes_{j=1}^{n}\left|\psi_{\theta_j}\right\rangle)_{AB} \otimes |extra\rangle\| &= O(n^2\epsilon) \\
\|UX_D^{(i)}|\psi'\rangle - \sigma^x_{D^{(i)}}(\bigotimes_{j=1}^{n}\left|\psi_{\theta_j}\right\rangle)_{AB} \otimes |extra\rangle\| &= O(n^2\epsilon) \\
\|UZ_D^{(i)}|\psi'\rangle - \sigma^z_{D^{(i)}}(\bigotimes_{j=1}^{n}\left|\psi_{\theta_j}\right\rangle)_{AB} \otimes |extra\rangle\| &= O(n^2\epsilon)\,,
\end{aligned}$$

where $D^{(i)}$ *is the ith qubit subsystem of* $(\mathbb{C}^2)_D^{\otimes n}$*, and* $\sigma^x_{D^{(i)}}$ *and* $\sigma^z_{D^{(i)}}$ *are Pauli operators acting on subsystem* $D^{(i)}$*.*

Proof: All the ingredients are already present in [16], and we only straighten out one small detail. We refer the reader to the the auxiliary results of Section A.3 for the precise statements of the Theorems from [16] (included as 34 and 35) and full detail.

Now, the operators $\{Z_i^{(k)}, X_i^{(k)}\}$ and V'_{n+i}, W'_{n+i} are defined just as in the ideal case of Subsection A.2, and from the latter also Z'_{n+i} and X'_{n+i}, in the same way. Let S_i be the correlation value of the ith game, i.e. the LHS of equation (A.9) and let $S_i^{(k)}$ be given by the LHS of equation (A.10). Then, again, we have $S_i = \frac{1}{2^{n-1}}\sum_{k=1}^{2^{n-1}} S_i^{(k)}$.
Now, denote by $I_*^{(i)} = \sqrt{8+2\beta_i^2}$ the maximum violation achievable by S_i, then by hypothesis we have $S_i \geq I_*^{(i)} - \epsilon$ for every $i = 1, .., n$.
Then we *claim* that for each i there are at most $2^{n-3}-1$ values of k such that $S_i^{(k)} < I_*^{(i)} - 5\epsilon$.
Proof: Suppose for a contradiction there were at least 2^{n-3} values of k such that $S_i^{(k)} < I_*^{(i)} - 5\epsilon$. Then

$$\begin{aligned}
S_i &\leq \frac{1}{2^{n-1}}[(2^{n-1}-2^{n-3})I_*^{(i)} + 2^{n-3}(I_* - 5\epsilon)] \\
&= I_*^{(i)} - \frac{5}{4}\epsilon < I_*^{(i)} - \epsilon\,,
\end{aligned}$$

which is a contradiction. Hence for each i, there are at least $2^{n-2}+2^{n-3}+1$ values of k s.t. $S_i^{(k)} \geq I_*^{(i)} - 5\epsilon$. Again, mimicking Subsection A.1.2, let G_i be the set of such "good" values of k. By Lemma 51, the above implies that, $\forall k \in G_i$,

$$\begin{aligned}
\|Z_i^{(k)}|\psi\rangle - Z'_{n+i}|\psi\rangle\| &\leq O(\sqrt{\epsilon}) \\
\|\sin\theta_i X_i^{(k)}(I+Z'_{n+i})|\psi\rangle - \cos\theta_i X'_{n+i}(I-Z_i^{(k)})|\psi\rangle\| &\leq O(\sqrt{\epsilon}) \\
\|(Z_i^{(k)}X_i^{(k)} + X_i^{(k)}Z_i^{(k)})|\psi\rangle\| \leq O(\sqrt{\epsilon}) \qquad \|(Z'_{n+i}X'_{n+i} + X'_{n+i}Z'_{n+i})|\psi\rangle\| &\leq O(\sqrt{\epsilon})\,.
\end{aligned}$$

And now, by the same argument used in Subsection A.1.2, we deduce that $\forall i \neq j$ there must be at least one pair $(\bar{k}, \bar{l})$ of superscripts such that $[Z_i^{(\bar{k})}, Z_j^{(\bar{l})}] = 0$ with both $\bar{k} \in G_i$ and $\bar{l} \in G_j$, and similarly for the X, Z and X, X commutation.

By running the same calculations as in the ideal case of Subsection A.2.1, just by using triangle inequalities where we do not have exact relations, much like we did in Subsection A.1.2, we deduce that, $\forall i \neq j$,

$$\begin{aligned}
\|(Z_i^{(k)} Z_j^{(l)} - Z_j^{(l)} Z_i^{(k)}) \, |\psi\rangle \, \| &\leq O(\sqrt{\epsilon}) \\
\|(Z_i^{(k)} X_j^{(l)} - X_j^{(l)} Z_i^{(k)}) \, |\psi\rangle \, \| &\leq O(\sqrt{\epsilon}) \\
\|(X_i^{(k)} X_j^{(l)} - X_j^{(l)} X_i^{(k)}) \, |\psi\rangle \, \| &\leq O(\sqrt{\epsilon})
\end{aligned}$$

for all k, l such that $k \in G_i$ and $l \in G_j$.

Now, for each $i = 1, .., n$ pick a $k_i \in G_i$. Then our choice of operators is $\{X_i^{(k_i)}, Z_i^{(k_i)}, X'_{n+i}, Z'_{n+i}\}$ for $i = 1, .., n$. We have shown that these satisfy the hypothesis of Theorem 33 with $O(\sqrt{\epsilon})$ bound, and this implies that there exists a local isometry sending $|\psi\rangle$ to a state that is $O(n^2\sqrt{\epsilon})$-close to a product n tilted EPR pairs with angles θ_i, and maps the action of our choice of operators on $|\psi\rangle$ to that of Pauli operators appropriately. This concludes the proof of Theorem 32.

A.3 Auxiliary results

Proof of Proposition 8. We first prove the generalization to a self-test of two singlets. The leap to a self test for n singlets will be straightforward to see after that. Given a bipartite state $|\psi\rangle_{AB}$ and operators $\{X_A^{(1)}, Z_A^{(1)}; X_B^{(1)}, Z_B^{(1)}\}$ and $\{X_A^{(2)}, Z_A^{(2)}; X_B^{(2)}, Z_B^{(2)}\}$ satisfying the conditions of Proposition 8, we will construct an appropriate local unitary $U = U_A \otimes U_B$ that achieves the claim of the proposition.

The construction of the isometry generalizes the "SWAP isometry" method described in Section 3.3. The idea is to extract the entanglement from the unknown system AB into a known system of four qubits $A^{(1)}A^{(2)}B^{(1)}B^{(2)}$ by performing a circuit that would simply swap the content of A with that of $A^{(1)}A^{(2)}$ (if A were actually a system of two qubits) and similarly for B.

The explicit unitary U_A (or rather the part of it that matters when the ancilla qubit is in the state

$|0\rangle$) is then

$$\begin{aligned}
U_A &= \frac{1}{4}\Big[(I+Z_A^{(1)})\otimes|0\rangle\langle 0|_{A^{(1)}} + X_A^{(1)}(I-Z_A^{(1)})\otimes|1\rangle\langle 0|_{A^{(1)}}\Big] \\
&\quad\cdot\Big[(I+Z_A^{(2)})\otimes|0\rangle\langle 0|_{A^{(2)}} + X_A^{(2)}(I-Z_A^{(2)})\otimes|1\rangle\langle 0|_{A^{(2)}}\Big] \\
&= \frac{1}{4}\Big[(I+Z_A^{(1)})(I+Z_A^{(2)})\otimes|0\rangle\langle 0|_{A^{(1)}}\otimes|0\rangle\langle 0|_{A^{(2)}} \\
&\qquad + (I+Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})\otimes|0\rangle\langle 0|_{A^{(1)}}\otimes|1\rangle\langle 0|_{A^{(2)}} \\
&\qquad + X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})\otimes|1\rangle\langle 0|_{A^{(1)}}\otimes|0\rangle\langle 0|_{A^{(2)}} \\
&\qquad + X_A^{(1)}(I-Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})\otimes|1\rangle\langle 0|_{A^{(1)}}\otimes|1\rangle\langle 0|_{A^{(2)}}\Big].
\end{aligned}$$

U_B is then similarly defined. So, we have

$$\begin{aligned}
&U|\psi\rangle_{AB}|0000\rangle_{A^{(1)}B^{(1)}A^{(2)}B^{(2)}} = U_A\otimes U_B|\psi\rangle_{AB}|0000\rangle_{A^{(1)}B^{(1)}A^{(2)}B^{(2)}} \\
&= \frac{1}{16}\Big[(I+Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle|0000\rangle \\
&+ (I+Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})|\psi\rangle|0001\rangle \\
&+ (I+Z_A^{(1)})(I+Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle|0100\rangle \\
&+ (I+Z_A^{(1)})(I+Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})|\psi\rangle|0101\rangle \\
&+ (I+Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})(I+Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle|0010\rangle \\
&+ (I+Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})(I+Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})|\psi\rangle|0011\rangle \\
&+ (I+Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle|0110\rangle \\
&+ (I+Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})|\psi\rangle|0111\rangle \\
&+ X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle|1000\rangle \\
&+ X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})|\psi\rangle|1001\rangle \\
&+ X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle|1100\rangle \\
&+ X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})|\psi\rangle|1101\rangle \\
&+ X_A^{(1)}(I-Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})(I+Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle|1010\rangle \\
&+ X_A^{(1)}(I-Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})(I+Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})|\psi\rangle|1011\rangle \\
&+ X_A^{(1)}(I-Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle|1110\rangle \\
&+ X_A^{(1)}(I-Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})|\psi\rangle|1111\rangle\Big]. \qquad \text{(A.30)}
\end{aligned}$$

Now, if we had actual commutativity relations, rather then just commutativity on $|\psi\rangle$, it wouldn't

be hard to see that the expression above reduces to

$$
\begin{aligned}
&U\left|\psi\right\rangle_{AB}\left|0000\right\rangle_{A^{(1)}B^{(1)}A^{(2)}B^{(2)}} = \\
&\frac{1}{16}\Big[(I+Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(1)})(I+Z_B^{(2)})\left|\psi\right\rangle\left|0000\right\rangle \\
&+(I+Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})(I+Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})\left|\psi\right\rangle\left|0011\right\rangle \\
&+X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})(I+Z_B^{(2)})\left|\psi\right\rangle\left|1100\right\rangle \\
&+X_A^{(1)}(I-Z_A^{(1)})X_A^{(2)}(I-Z_A^{(2)})X_B^{(1)}(I-Z_B^{(1)})X_B^{(2)}(I-Z_B^{(2)})\left|\psi\right\rangle\left|1111\right\rangle\,, \qquad \text{(A.31)}
\end{aligned}
$$

i.e. the only the terms to survive are the ones in which the subsystems $A^{(1)}$, $B^{(1)}$ have the same value for their qubit, and so do subsystems $A^{(2)}$,$B^{(2)}$. This is because

$$
\begin{aligned}
(I-Z_A^{(1)})(I+Z_B^{(1)})\left|\psi\right\rangle &= (I-Z_A^{(1)})(I+Z_A^{(1)})\left|\psi\right\rangle \qquad && \text{since } Z_A^{(1)}\left|\psi\right\rangle = Z_B^{(1)}\left|\psi\right\rangle \\
&= \left(I-(Z_A^{(1)})^2\right)\left|\psi\right\rangle = 0 \qquad && \text{since} (Z_A^{(1)})^2 = I
\end{aligned}
$$

and similar other expressions.

The above result holds, in fact, also when the commutativity relations are only on $\left|\psi\right\rangle$. The reason for this is the following. Operators on A and operators on B always commute with each other, and notice that we can transform operators on A into operators on B and viceversa (if they are immediately in front of $\left|\psi\right\rangle$) using the relations $Z_A^{(i)}\left|\psi\right\rangle = Z_B^{(i)}\left|\psi\right\rangle$ and $X_A^{(i)}\left|\psi\right\rangle = X_B^{(i)}\left|\psi\right\rangle$. So for instance, if we look at the term corresponding to $\left|1000\right\rangle$ in (A.30), we have (spelling out the calculation for the sake of clarity):

$$
\begin{aligned}
&X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(1)})(I+Z_B^{(2)})\left|\psi\right\rangle \\
&= X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(2)})(I+Z_B^{(1)})\left|\psi\right\rangle \quad \text{using } Z_B^{(1)}Z_B^{(2)}\left|\psi\right\rangle = Z_B^{(2)}Z_B^{(1)}\left|\psi\right\rangle \\
&= (I+Z_B^{(2)})(I+Z_B^{(1)})X_A^{(1)}(I-Z_A^{(1)})(I+Z_A^{(2)})\left|\psi\right\rangle \\
&= (I+Z_B^{(2)})(I+Z_B^{(1)})X_A^{(1)}(I+Z_A^{(2)})(I-Z_A^{(1)})\left|\psi\right\rangle \quad \text{using } Z_A^{(1)}Z_A^{(2)}\left|\psi\right\rangle = Z_A^{(2)}Z_A^{(1)}\left|\psi\right\rangle \\
&= (I+Z_B^{(2)})(I+Z_B^{(1)})X_A^{(1)}(I+Z_A^{(2)})(I-Z_B^{(1)})\left|\psi\right\rangle \quad \text{using } Z_A^{(1)}\left|\psi\right\rangle = Z_B^{(1)}\left|\psi\right\rangle \\
&= (I+Z_B^{(2)})(I+Z_B^{(1)})(I-Z_B^{(1)})X_A^{(1)}(I+Z_A^{(2)})\left|\psi\right\rangle \quad \text{since operators on A and B commute} \\
&= (I+Z_B^{(2)})(I+Z_B^{(1)})(I-Z_B^{(1)})(I+Z_A^{(2)})X_A^{(1)}\left|\psi\right\rangle \quad \text{using } X_A^{(1)}Z_A^{(2)}\left|\psi\right\rangle = Z_A^{(2)}X_A^{(1)}\left|\psi\right\rangle \\
&= (I+Z_B^{(2)})(I+Z_B^{(1)})(I+Z_A^{(2)})X_A^{(1)}(I-Z_B^{(1)})\left|\psi\right\rangle \\
&= (I+Z_B^{(2)})(I+Z_B^{(1)})(I+Z_A^{(2)})X_A^{(1)}(I-Z_A^{(1)})\left|\psi\right\rangle \quad \text{again using } Z_A^{(1)}\left|\psi\right\rangle = Z_B^{(1)}\left|\psi\right\rangle \\
&= (I+Z_B^{(2)})(I+Z_A^{(2)})X_A^{(1)}(I-Z_A^{(1)})(I+Z_B^{(1)})\left|\psi\right\rangle \\
&= (I+Z_B^{(2)})(I+Z_A^{(2)})X_A^{(1)}(I-(Z_A^{(1)})^2)\left|\psi\right\rangle \\
&= 0\,.
\end{aligned}
$$

It is clear, then, that using this technique we can permute the order of the operators on A at our will, and similarly for those on B. And since operators on A and B commute with each other, we can essentially permute all operators. Hence, for the purpose of our analysis, commutation relations on $|\psi\rangle$ behave exactly as commutation relations on the whole space. Hence, going back to equation (A.31), it is not difficult to see, using the ability to permute operators and the fact that $X_A^{(i)}|\psi\rangle = X_B^{(i)}|\psi\rangle \Rightarrow X_A^{(i)} X_B^{(i)}|\psi\rangle = |\psi\rangle$, that

$$
\begin{aligned}
&U|\psi\rangle_{AB}|0000\rangle_{A^{(1)}B^{(1)}A^{(2)}B^{(2)}} \\
&= \frac{1}{16}(I+Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle_{AB} \otimes \big(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\big) \\
&= |extra\rangle_{AB} \left|\Phi^+\right\rangle^{\otimes 2}_{A^{(1)}B^{(1)}A^{(2)}B^{(2)}} ,
\end{aligned}
$$

where $|extra\rangle_{AB} = (I+Z_A^{(1)})(I+Z_A^{(2)})(I+Z_B^{(1)})(I+Z_B^{(2)})|\psi\rangle_{AB}$ up to normalization. This completes the proof for the case $n = 2$.

It is straightforward to see that the proof for arbitrary n follows in a very similar way. The unitary (or rather the part of it that matters) naturally becomes $U = U_A \otimes U_B$ with

$$U_A = \frac{1}{2^n}\prod_{i=1}^{n}\Big[(I+Z_A^{(i)})\otimes|0\rangle\langle 0|_{A^{(i)}} + X_A^{(i)}(I-Z_A^{(i)})\otimes|1\rangle\langle 0|_{A^{(i)}}\Big]$$

and U_B similarly defined.

It is easy to convince oneself that the order of all operators can be permuted at will, just like it was possible for $n = 2$. Just as in the case $n = 2$, the only terms that don't vanish in $U|\psi\rangle_{AB}|0\rangle^{\otimes n}_{A^{(1)}B^{(1)}A^{(2)}B^{(2)}..A^{(n)}B^{(n)}}$ are the 2^n terms in which each pairs of subsystems/qubits $A^{(i)}$, $B^{(i)}$ have the same value (either both 0 or both 1). As one expects, the $|extra\rangle_{AB}$ state we end up with is, up to normalization,

$$|extra\rangle_{AB} = \prod_{i=1}^{n}(I+Z_A^{(i)})(I+Z_B^{(i)})|\psi\rangle_{AB} .$$

The proof of equation (A.7) also follows without difficulty. □

Proof of Proposition 9: Given a bipartite state $|\psi\rangle_{AB}$ and operators $\{Z_i^{(1)}, X_i^{(1)}; Z'_{n+i}, X'_{n+i} : i = 1,..,n\}$ satisfying the conditions of Proposition 9, we will show how to construct an appropriate local unitary $U = U_A \otimes U_B$ that achieves the claim of the proposition.

Again, the unitary is just a "SWAP" from the unknown system A to a system of n qubits $A^{(1)}..A^{(n)}$ and similarly for B. It is defined in exactly the same way as in the case of maximally entangled qubits. We then apply the local unitary to the state $|\psi\rangle_{AB}\otimes|0\rangle^{\otimes n}_{A^{(1)}B^{(1)}A^{(2)}B^{(2)}..A^{(n)}B^{(n)}}$. We obtain a sum that includes all terms in the computational basis. For the terms such that for some i the values

on subsystems A^i and B^i are different, let i_* be the largest such index (i.e. the one whose operators are further to the right). Then we can commute the operators corresponding to i_* all the way to the right (in this case the operators are $X_A^{i_*}(I - Z_A^{i_*})(I + Z_B^{i_*})$, or this with A and B swapped) since to the right of these there are only Z operators, and so we can apply the same commutation trick that we used in the proof of 8. But $X_A^{i_*}(I - Z_A^{i_*})(I + Z_B^{i_*}) |\psi\rangle = 0$ simply because terms like this vanish even in the case $n = 1$, for which we know that the unitary works [102].

For the terms in which the values on subsystems $A^{(i)}$ and $B^{(i)}$ are equal for all i, we know, from the proof of the case $n = 1$ in [102], that

$$\frac{1}{4}(I + Z_A^{(i)})(I + Z_B^{(i)}) |\psi\rangle = \frac{(I + Z_A^{(i)})}{2} |\psi\rangle \qquad \text{(this is the 00 case)}$$
$$X_A^{(i)}(I - Z_A^{(i)})X_B^{(i)}(I - Z_B^{(i)}) |\psi\rangle = \tan\theta_i \frac{(I + Z_A^{(i)})}{2} |\psi\rangle \qquad \text{(this is the 11 case).}$$

Thus, if we factor out a $\frac{1}{\cos\theta_i}$, we see that a "00" term contributes a factor of $\cos\theta_i$, while a "11" term contributes a factor of $\sin\theta_i$, which is precisely what we need.
Hence, we conclude that

$$U |\psi\rangle_{AB} \otimes |0\rangle^{\otimes n}_{A^{(1)}B^{(1)}A^{(2)}B^{(2)}..A^{(n)}B^{(n)}}$$
$$= |extra\rangle \otimes \bigotimes_{i=1}^{n} \left(\cos\theta_i |00\rangle + \sin\theta_i |11\rangle \ , \right)$$

where $|extra\rangle = \prod_{i=1}^{n}(I + Z_A^{(i)}) |\psi\rangle_{AB}$ up to normalization.

We state, here, the Theorems from [16] that, upon fixing one detail, with the help of Lemma 52 from [72], directly imply the Theorems (30 and 33) that we used in subsections (A.1.2) and (A.2.2) to deduce the existence of the desired isometries, with robustness, from the operators we constructed in the "non-tilted" and in the tilted case respectively. For the proofs of these Theorems we refer the reader to their original source [16].

Merging the hypothesis of Theorem 2.1 and the conclusions of Corollary 2.2 from [16], we can state the following:

Theorem 34. *([16]) Let $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state. Suppose there are reflections $\{X_A^{(i)}, Z_A^{(i)}; X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$ acting on subsystems A and B respectively, such that, for D either A or B and for all $i \neq j$, they satisfy $\{X_D^{(i)}, Z_D^{(i)}\} = 0$ and*

$$\| M_A^{(i)} |\psi\rangle - M_B^{(i)} |\psi\rangle \| \leq \epsilon$$
$$\| [M_D^{(i)}, N_D^{(j)}] |\psi\rangle \| \leq \epsilon \, ,$$

where $M, N \in \{X, Z\}$.
Then, letting $|\psi'\rangle = |\psi\rangle \otimes |\Phi^+\rangle_{A'}^{\otimes n} \otimes |\Phi^+\rangle_{B'}^{\otimes n} \in \mathcal{H}_A \otimes (\mathbb{C}^2)_{A'}^{\otimes 2n} \otimes \mathcal{H}_B \otimes (\mathbb{C}^2)_{B'}^{\otimes 2n}$, there exist a local unitary $U = U_A \otimes U_B$ where $U_D : \mathcal{H}_D \otimes (\mathbb{C}^2)_{D'}^{\otimes 2n} \to (\mathbb{C}^2)_D^{\otimes n} \otimes \hat{\mathcal{H}}_D$ and a state $|extra\rangle \in \hat{\mathcal{H}}_A \otimes \hat{\mathcal{H}}_B$ such that $\forall i$

$$\begin{aligned} \| U |\psi'\rangle - |\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle \| &= O(n^{\frac{3}{2}}\epsilon) \\ \| U X_D^{(i)} |\psi'\rangle - \sigma^x_{D^{(i)}} |\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle \| &= O(n^{\frac{3}{2}}\epsilon) \qquad \text{(A.32)} \\ \| U Z_D^{(i)} |\psi'\rangle - \sigma^z_{D^{(i)}} |\Phi^+\rangle_{AB}^{\otimes n} \otimes |extra\rangle \| &= O(n^{\frac{3}{2}}\epsilon)\,, \qquad \text{(A.33)} \end{aligned}$$

where $D^{(i)}$ is the ith qubit subsystem of $(\mathbb{C}^2)_D^{\otimes n}$, and $\sigma^x_{D^{(i)}}$ and $\sigma^z_{D^{(i)}}$ are Pauli operators acting on subsystem $D^{(i)}$.

Note that we have adapted notation in the original statement to fit ours. And we also applied an extra triangle inequality to obtain equations (A.32) and (A.33).

In a nutshell, Theorem 34 says that given operators satisfying its hypothesis, there exists an isometry, which adds an extra ancilla state to both Alice's and Bob's systems, namely n EPR pairs for each of Alice and Bob, which maps the unknown quantum state to a state that is close to a tensor product of n EPR pairs between Alice and Bob, and maps the action of the unknown operators on $|\psi\rangle$ to that of Pauli operators accordingly. Note that the ancilla EPR pairs are not shared between Alice and Bob, but each of the two provers has n EPR pairs separately.
The only difference between Theorem 30 in Subsection A.1.2 and the Theorem we just stated is that the latter requires exact anticommutation between X and Z operators on the same side corresponding to the same superscript, while the former requires just approximate anticommutation when acting on $|\psi\rangle$. We will show how to bridge this gap by using Lemma 52 stated below, from [72].

The following result, is the generalisation of the Theorem above to tilted EPR pairs, and we state it by combining the hypothesis of Theorem A.1 from [16] and the conclusions of Corollary A.3 from [16]. The robustness bound is slightly worse than that of Theorem 34 stated above.

Theorem 35. *([16]) Let $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state. Suppose there are reflections $\{X_A^{(i)}, Z_A^{(i)}; X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$ acting on subsystems A and B respectively, such that, for D either A or B and for all $i \neq j$, they satisfy $\{X_D^{(i)}, Z_D^{(i)}\} = 0$ and, for some angles θ_i, $i = 1, .., n$,*

$$\begin{aligned} \| Z_A^{(i)} |\psi\rangle - Z_B^{(i)} |\psi\rangle \| &\leq \epsilon \qquad \text{(A.34)} \\ \| \sin\theta_i X_A^{(i)} (I + Z_B^{(i)}) |\psi\rangle - \cos\theta_i X_B^{(i)} (I - Z_A^{(i)}) |\psi\rangle \| &\leq \epsilon \qquad \text{(A.35)} \\ \| [M_D^{(i)}, N_D^{(j)}] |\psi\rangle \| &\leq \epsilon\,, \end{aligned}$$

where $M, N \in \{X, Z\}$. *Then, letting* $|\psi'\rangle = |\psi\rangle \otimes \left(\bigotimes_{i=1}^{n} |\psi_{\theta_i}\rangle\right)_{A'} \otimes \left(\bigotimes_{i=1}^{n} |\psi_{\theta_i}\rangle\right)_{B'} \in \mathcal{H}_A \otimes (\mathbb{C}^2)^{\otimes 2n}_{A'} \otimes \mathcal{H}_B \otimes (\mathbb{C}^2)^{\otimes 2n}_{B'}$, *there exist a local unitary* $U = U_A \otimes U_B$ *where* $U_D : \mathcal{H}_D \otimes (\mathbb{C}^2)^{\otimes 2n}_{D'} \to (\mathbb{C}^2)^{\otimes n}_{D} \otimes \hat{\mathcal{H}}_D$ *and a state* $|extra\rangle \in \hat{\mathcal{H}}_A \otimes \hat{\mathcal{H}}_B$ *such that, for all i,*

$$\|U|\psi'\rangle - \left(\bigotimes_{j=1}^{n} \left|\psi_{\theta_j}\right\rangle\right)_{AB} \otimes |extra\rangle\| = O(n^2\epsilon)$$

$$\|UX_D^{(i)}|\psi'\rangle - \sigma^x_{D^{(i)}}\left(\bigotimes_{j=1}^{n} \left|\psi_{\theta_j}\right\rangle\right)_{AB} \otimes |extra\rangle\| = O(n^2\epsilon)$$

$$\|UZ_D^{(i)}|\psi'\rangle - \sigma^z_{D^{(i)}}\left(\bigotimes_{j=1}^{n} \left|\psi_{\theta_j}\right\rangle\right)_{AB} \otimes |extra\rangle\| = O(n^2\epsilon)\,,$$

where $D^{(i)}$ *is the ith qubit subsystem of* $(\mathbb{C}^2)^{\otimes n}_D$, *and* $\sigma^x_{D^{(i)}}$ *and* $\sigma^z_{D^{(i)}}$ *are Pauli operators acting on subsystem* $D^{(i)}$.

Here the isometry adds an extra ancilla state of n tilted EPR pairs on Alice's side and n on Bob's side, with the appropriate angles. Again, note that these ancilla tilted pairs are not shared between Alice and Bob, but they each have n separately (as stated in [16], the angles θ_i are all equal; however, the theorem is easily seen to hold true also when the θ_i are different). Again, this Theorem requires exact anticommutation between X, Z operators with the same superscript, while 33 that we used in Subsection A.2.2 requires just approximate anticommutation when acting on $|\psi\rangle$. So, we can almost apply theorems 34 and 35 directly to our analysis, except that for the set of operators that we construct in subsections A.1.2 and A.2.2 the anticommutation that we achieve is only approximate. The following Lemma, from [72], helps bridge this gap.

Lemma 52. *([16] [72]) Let* X, Z *be balanced reflections on a space of even dimension* $\mathcal{H}_A$, *and let* $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ *be such that* $\|\{X, Z\} \otimes I|\psi\rangle\| \leq \epsilon$. *Then there exists a balanced reflection* Z' *on* $\mathcal{H}$ *such that* $\{X, Z'\} = 0$ *and* $\|(Z - Z') \otimes I|\psi\rangle\| \leq \sqrt{3/2}\epsilon$.

Now, we just need to show that Theorem 34 and Lemma 52 imply Theorem 30, and that Theorem 35 and Lemma 52 imply Theorem 33. The only detail that we need to take care of in order to do so is the following. As we have mentioned earlier, the hypotheses of Theorems 30 and 33 are the same as those of Theorems 34 and 35 respectively, except for the fact that the anticommutation required between X, Z operators with the same superscripts in the latter is exact. Now, given operators satisfying the hypothesis of Theorem 30 (or Theorem 33), we can make use of Lemma 52 to replace the operators $\{Z_D^{(i)}\}_{i=1,..,n}$ with operators $\{Z_D^{\prime(i)}\}_{i=1,..,n}$ such that the exact anticommutation conditions hold, and the existence of these is guaranteed by Lemma 52. However, in order to apply Theorem 34 (or Theorem 35) to the new set of operators, we need to check that this still satisfies all other conditions in the hypothesis (most of them are immediate). We will do this check for the tilted

version (Theorems 33 and 35), and then the "non-tilted" version follows, being just a particular case.

Claim 2. *Suppose that* $|\psi\rangle$ *and the set of operators* $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$ *satisfy the hypothesis of Theorem 33 with bound* ϵ*. For each* $i = 1,..n$*, and for* D *either* A *or* B*, let* $Z_D^{\prime(i)}$ *be reflections such that* $\{X_D^{(i)}, Z_D^{\prime(i)}\} = 0$ *and* $\|(Z_D^{(i)} - Z_D^{\prime(i)})\,|\psi\rangle\,\| \leq \epsilon$*. The existence of such operators* $Z_D^{\prime(i)}$ *is guaranteed by Lemma 52. Then,* $|\psi\rangle$*, together with the new set of operators* $\{X_A^{(i)}, Z_A^{\prime(i)}, X_B^{(i)}, Z_B^{\prime(i)}\}_{i=1,..,n}$ *satisfies the hypothesis of Theorem 35.*

Proof. Conditions (A.34) and (A.35) of Theorem 35 hold for the new operators by applying triangle inequalities, the fact that $X_A^{(i)}$ and $X_B^{(i)}$ are unitary and that $\|(Z_D^{(i)} - Z_D^{\prime(i)})\,|\psi\rangle\,\| \leq \epsilon$. Next, we need to check that the commutation between operators on the same side with different superscripts still holds for the new operators. Obviously, commutation between X operators holds as we haven't changed those.

For Z, Z commutation, we have $\|Z_A^{\prime(i)} Z_A^{\prime(j)}\,|\psi\rangle - Z_A^{\prime(j)} Z_A^{\prime(i)}\,|\psi\rangle\,\| \approx \|Z_A^{\prime(i)} Z_A^{(j)}\,|\psi\rangle - Z_A^{\prime(j)} Z_A^{(i)}\,|\psi\rangle\,\| \approx \|Z_A^{\prime(i)} Z_B^{(j)}\,|\psi\rangle - Z_A^{\prime(j)} Z_B^{(i)}\,|\psi\rangle\,\| \approx \|Z_B^{(j)} Z_A^{(i)}\,|\psi\rangle - Z_B^{(i)} Z_A^{(j)}\,|\psi\rangle\,\| \approx \|Z_A^{(i)} Z_A^{(j)}\,|\psi\rangle - Z_A^{(j)} Z_A^{(i)}\,|\psi\rangle\,\| = O(\epsilon)$, where the approximate equalities are up to an $O(\epsilon)$ error brought by the application of triangle inequalities. Recall that both Z and Z' are reflections and, hence, unitary. The second approximate equality is by condition (A.28), and the final equality is by hypothesis.

X, Z commutation is slightly more involved. We have

$$
\begin{aligned}
&\|Z_A^{\prime(i)} X_A^{(j)}\,|\psi\rangle - X_A^{(j)} Z_A^{\prime(i)}\,|\psi\rangle\,\| \\
&\approx \|\frac{1}{2}(I + Z_B^{(j)}) Z_A^{\prime(i)} X_A^{(j)}\,|\psi\rangle + \frac{1}{2}(I - Z_B^{(j)}) Z_A^{\prime(i)} X_A^{(j)} - X_A^{(j)} Z_A^{(i)}\,|\psi\rangle\,\| \\
&\approx \|\frac{1}{2}\cot(\theta_j) Z_A^{\prime(i)} X_B^{(j)} (I - Z_B^{(j)})\,|\psi\rangle + \frac{1}{2}\tan(\theta_j) Z_A^{\prime(i)} X_B^{(j)} (I + Z_B^{(j)}) - X_A^{(j)} Z_A^{(i)}\,|\psi\rangle\,\| \\
&\approx \|\frac{1}{2}\cot(\theta_j) Z_A^{(i)} X_B^{(j)} (I - Z_B^{(j)})\,|\psi\rangle + \frac{1}{2}\tan(\theta_j) Z_A^{(i)} X_B^{(j)} (I + Z_B^{(j)}) - X_A^{(j)} Z_A^{(i)}\,|\psi\rangle\,\| \\
&\approx \|\frac{1}{2} Z_A^{(i)} X_A^{(j)} (I + Z_B^{(j)})\,|\psi\rangle + \frac{1}{2} Z_A^{(i)} X_A^{(j)} (I - Z_B^{(j)}) - X_A^{(j)} Z_A^{(i)}\,|\psi\rangle\,\| \\
&\approx \|Z_A^{(i)} X_A^{(j)}\,|\psi\rangle - X_A^{(j)} Z_A^{(i)}\,|\psi\rangle\,\| = O(\epsilon)\,.
\end{aligned}
$$

The second approximate equality follows by Equation (A.29).

Hence, we have shown that the new set of operators $\{X_A^{(i)}, Z_A^{\prime(i)}, X_B^{(i)}, Z_B^{\prime(i)}\}_{i=1,..,n}$, indeed, satisfies the hypothesis of Theorem 35. □

It follows, then, under the hypothesis of Claim 2, that the conclusion of Theorem 35 holds for $|\psi\rangle$ and the operators $\{X_A^{(i)}, Z_A^{\prime(i)}, X_B^{(i)}, Z_B^{\prime(i)}\}_{i=1,..,n}$. But it is clear that if this holds for $|\psi\rangle$

together with the new set of operators, then it also holds for $|\psi\rangle$ together with the original set of operators $\{X_A^{(i)}, Z_A^{(i)}, X_B^{(i)}, Z_B^{(i)}\}_{i=1,..,n}$, simply by applying a few triangle inequalities. Notice that the conclusion of Theorem 35 is the same as that of Theorem 33 (just the hypothesis of the former is stricter). This completes the proof of Theorem 33.

Appendix B

APPENDIX FOR "ALL PURE BIPARTITE ENTANGLED STATES CAN BE SELF-TESTED"

B.1 Proof of Lemma 37

In this section, we provide a proof of Lemma 37. We explicitly construct a local isometry Φ such that $\Phi(|\psi\rangle) = |\text{extra}\rangle \otimes |\psi_{\text{target}}\rangle$, where the ideal target state is $|\psi_{\text{target}}\rangle = \sum_{i=0}^{d-1} c_i |ii\rangle$, and $|\text{extra}\rangle$ is some auxiliary state.

Proof. Recall that $\{P_A^{(k)}\}$ is a complete orthogonal set of orthogonal projections by hypothesis. Then, notice that for $i \neq j$ we have, using condition (5.1), $P_B^{(i)} P_B^{(j)} |\psi\rangle = P_B^{(i)} P_A^{(j)} |\psi\rangle = P_A^{(j)} P_A^{(i)} |\psi\rangle = 0$, i.e the $P_B^{(k)}$ are "orthogonal when acting on $|\psi\rangle$". Then, we can invoke a variation of the *orthogonalization lemma* (Lemma 21 from Kempe and Vidick [51]) to obtain projections on Bob's side that are exactly orthogonal, and have the same action on $|\psi\rangle$.

Lemma 53. *Let ρ be a density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$. Let $P_1, \ldots, P_k$ be projections on $\mathcal{H}_B$ such that, for all $i \neq j$,*

$$\sum_{i \neq j} \text{Tr}\big[I \otimes P_i P_j P_i \rho\big] \leq \epsilon\,.$$

Then, there exist orthogonal projections $Q_1, \ldots, Q_k$ on $\mathcal{H}_B$ such that

$$\sum_{i=1}^{k} \text{Tr}\left[I \otimes (P_i - Q_i)^2 \rho\right] = O\big(\epsilon^{\frac{1}{2}}\big)\,.$$

Kempe and Vidick only considered the case of finite-dimensional Hilbert spaces. When we apply the self-testing results of Chapter 5 to obtain the non-closure of the set of quantum correlations in Chapter 6 (corollary 7), we need our self-testing results to hold (in the exact case) when Alice and Bob's Hilbert spaces are possibly infinite-dimensional (and separable). To clarify, the self-tested state will still be finite-dimensional, but we will not assume that Alice and Bob's starting Hilbert spaces are finite-dimensional. Here, we provide a simple proof of the exact version of Lemma 53 (i.e. $\epsilon = 0$), in the case of infinite-dimensional, separable Hilbert spaces.

Proof of Lemma 53 (for $\epsilon = 0$ and infinite-dimensional, separable Hilbert spaces). Let $\rho_B = \text{Tr}_A[\rho]$. Let $\text{supp}(\rho_B) = \text{Ker}(\rho_B)^{\perp}$. For $i \in \{1, .., k\}$, define Q_i to be the projection onto $P_i \,\text{supp}(\rho_B) = \{P_i |v\rangle : |v\rangle \in \text{supp}(\rho_B)\}$. By the spectral theorem, since ρ_B is compact and self-adjoint, there is an orthonormal basis of $\text{supp}(\rho_B)$ consisting of eigenvectors of ρ_B with non-zero

eigenvalues. Together with the fact that, by definition, $P_i |v\rangle = Q_i |v\rangle$ for all $|v\rangle \in \mathrm{supp}(\rho_B)$, this straightforwardly implies that

$$\mathrm{Tr}\left[I \otimes (P_i - Q_i)^2 \rho\right] = 0.$$

Notice that $\mathrm{Tr}\left[P_i P_j P_i \rho_B\right] = \mathrm{Tr}\left[I \otimes P_i P_j P_i \rho\right] = 0$ for any $i \neq j$, where the last equality is by hypothesis. This implies $P_j |v\rangle = 0$ for any $|v\rangle \in P_i \,\mathrm{supp}(\rho_B)$ (where this is again seen via the spectral decomposition of ρ_B). It follows that $|v\rangle \perp P_j \,\mathrm{supp}(\rho_B)$ for any $|v\rangle \in P_i \,\mathrm{supp}(\rho_B)$, which, by definition of Q_j, implies that $Q_j |v\rangle = 0$. Since $Q_i |v\rangle = 0$ for any $v \in (P_i \,\mathrm{supp}\,(\rho_B))^\perp$, we deduce that $Q_j Q_i |v\rangle$ for any $|v\rangle$. Similarly, one shows that $Q_i Q_j |v\rangle$ for any $|v\rangle$, which implies that Q_i and Q_j are orthogonal, as desired. □

Applying Lemma 53, yields a new set of orthogonal projections $\{\tilde{P}_B^{(k)}\}$ on Bob's side such that $\tilde{P}_B^{(k)} |\psi\rangle = P_B^{(k)} |\psi\rangle$ for all k.

Now, define $Z_A := \sum_{k=0}^{d-1} \omega^k P_A^{(k)}$ and $Z_B := \sum_{k=0}^{d-1} \omega^k \tilde{P}_B^{(k)} + \mathbb{1} - \sum_{k=0}^{d-1} \tilde{P}_{A/B}^{(k)}$. In particular, Z_A and Z_B are unitary. Notice, moreover, that $\left(\mathbb{1} - \sum_{k=0}^{d-1} \tilde{P}_{A/B}^{(k)}\right) |\psi\rangle = 0$, again using condition (5.1).

Define the local isometry

$$\Phi := (R_{AA'} \otimes R_{BB'})(\bar{F}_{A'} \otimes \bar{F}_{B'})(S_{AA'} \otimes S_{BB'})(F_{A'} \otimes F_{B'}),$$

where F is the quantum Fourier transform, $\bar{F}$ is the inverse quantum Fourier transform, $R_{AA'}$ is defined so that $|\phi\rangle_A |k\rangle_{A'} \mapsto X_A^{(k)} |\phi\rangle_A |k\rangle_{A'} \;\; \forall |\phi\rangle$, and similarly for $R_{BB'}$, and $S_{AA'}$ is defined so that $|\phi\rangle_A |k\rangle_{A'} \mapsto Z_A^k |\phi\rangle_A |k\rangle_{A'} \;\; \forall |\phi\rangle$, and similarly for $S_{BB'}$. We compute the action of Φ on $|\psi\rangle_{AB} |0\rangle_{A'} |0\rangle_{B'}$. For ease of notation, we drop the tildes from the $\tilde{P}_B^{(k)}$, while still referring to the new orthogonal projections.

$$\begin{aligned}
|\psi\rangle_{AB} |0\rangle_{A'} |0\rangle_{B'} &\xrightarrow{F_{A'} \otimes F_{B'}} \frac{1}{d} \sum_{k,k'} |\psi\rangle_{AB} |k\rangle_{A'} |k'\rangle_{B'} \\
&\xrightarrow{S_{AA'} \otimes S_{BB'}} \frac{1}{d} \sum_{k,k'} \left(\sum_j \omega^j P_A^{(j)}\right)^k \left(\sum_{j'} \omega^{j'} P_B^{(j')} + \mathbb{1} - \sum_k P_B^{(j')}\right)^{k'} |\psi\rangle_{AB} |k\rangle_{A'} |k'\rangle_{B'} \\
&= \frac{1}{d} \sum_{k,k',j,j'} \omega^{jk} \omega^{j'k'} P_A^{(j)} P_B^{(j')} |\psi\rangle_{AB} |k\rangle_{A'} |k'\rangle_{B'} \\
&= \frac{1}{d} \sum_{k,k',j,j'} \omega^{jk} \omega^{j'k'} P_A^{(j)} P_A^{(j')} |\psi\rangle_{AB} |k\rangle_{A'} |k'\rangle_{B'} \\
&= \frac{1}{d} \sum_{k,k',j} \omega^{j(k+k')} P_A^{(j)} |\psi\rangle_{AB} |k\rangle_{A'} |k'\rangle_{B'}
\end{aligned}$$

$$
\begin{aligned}
&\xrightarrow{\bar{F}_{A'}\otimes\bar{F}_{B'}} \frac{1}{d^2}\sum_{k,k',j,l,l'} \omega^{j(k+k')}\omega^{-lk}\omega^{-l'k'} P_A^{(j)} \left|\psi\right\rangle_{AB} \left|l\right\rangle_{A'} \left|l'\right\rangle_{B'} \\
&\quad = \frac{1}{d^2}\sum_{k,k',j,l,l'} \omega^{k(j-l)}\omega^{k'(j-l')} P_A^{(j)} \left|\psi\right\rangle_{AB} \left|l\right\rangle_{A'} \left|l'\right\rangle_{B'} \\
&\quad = \sum_j P_A^{(j)} \left|\psi\right\rangle_{AB} \left|j\right\rangle_{A'} \left|j\right\rangle_{B'} \qquad \text{(B.1)} \\
&\xrightarrow{R_{AA'}\otimes R_{BB'}} \sum_j X_A^{(j)} X_B^{(j)} P_A^{(j)} \left|\psi\right\rangle_{AB} \left|j\right\rangle_{A'} \left|j\right\rangle_{B'} \\
&\quad = \sum_j \frac{c_j}{c_0} P_A^{(0)} \left|\psi\right\rangle_{AB} \left|j\right\rangle_{A'} \left|j\right\rangle_{B'} \\
&\quad = \frac{1}{c_0} P_A^{(0)} \left|\psi\right\rangle_{AB} \otimes \sum_j c_j \left|j\right\rangle_{A'} \left|j\right\rangle_{B'} \\
&\quad = \left|\text{extra}\right\rangle \otimes \left|\psi_{\text{target}}\right\rangle \ .
\end{aligned}
$$

□

It is an easy check to see that the whole proof above can be repeated by starting from a mixed joint state, yielding a corresponding version of the Lemma that holds for a general mixed state.

B.2 Self-testing the measurements

Not much work is required to extend self-testing to the measurement operators, using the same local isometry Φ, defined via the projections $P_{A/B}^{(k)}$ and the unitary operators $Z_{A/B}$ and $X_{A/B}^{(k)}$, as defined in the main text.

Consider $\hat{A}_{x,m} = \Pi_{2m}^{A_x} - \Pi_{2m+1}^{A_x}$ and $\hat{B}_{y,m} = \Pi_{2m}^{B_y} - \Pi_{2m+1}^{B_y}$. Let $A_{x,m}$,$B_{y,m}$ be the two-qubit ideal measurements achieving maximal violation of tilted CHSH on the (2m,2m+1) subspace, i.e. $A_{0,m} = [\sigma_Z]_m$, $A_{1,m} = [\sigma_X]_m$, $B_{0,m} = [\cos(\mu_m)\sigma_Z + \sin(\mu_m)\sigma_X]_m$, $B_{1,m} = [\cos(\mu_m)\sigma_Z - \sin(\mu_m)\sigma_X]_m$, with the notation from Subsection 5.1.2.3. We claim first that $\Phi(\hat{A}_{x,m}\left|\psi\right\rangle) = \left|\text{extra}\right\rangle \otimes A_{x,m}\left|\psi_{\text{target}}\right\rangle$ and $\Phi(\hat{B}_{y,m}\left|\psi\right\rangle) = \left|\text{extra}\right\rangle \otimes B_{y,m}\left|\psi_{\text{target}}\right\rangle$.

Following closely the proof in Appendix B.1 up to Equation (B.1), we have

$$
\begin{aligned}
&\Phi(\hat{A}_{x,m}\left|\psi\right\rangle) = R_{AA'} \otimes R_{BB'} \sum_j P_B^{(j)} \hat{A}_{x,m} \left|\psi\right\rangle_{AB} \left|j\right\rangle_{A'} \left|j\right\rangle_{B'} \\
=&R_{AA'} \otimes R_{BB'} \Big(P_B^{(2m)} \hat{A}_{x,m} \left|\psi\right\rangle_{AB} \left|2m\right\rangle_{A'} \left|2m\right\rangle_{B'} + P_B^{(2m+1)} \hat{A}_{x,m} \left|\psi\right\rangle_{AB} \left|2m+1\right\rangle_{A'} \left|2m+1\right\rangle_{B'} \Big) \\
=&X_B^{(2m)} X_A^{(2m)} P_B^{(2m)} \hat{A}_{x,m} \left|\psi\right\rangle_{AB} \left|2m\right\rangle_{A'} \left|2m\right\rangle_{B'} \\
&+ X_B^{(2m+1)} X_A^{(2m+1)} P_B^{(2m+1)} \hat{A}_{x,m} \left|\psi\right\rangle_{AB} \left|2m+1\right\rangle_{A'} \left|2m+1\right\rangle_{B'} \\
=&X_B^{(2m)} X_A^{(2m)} \Big(P_B^{(2m)} \hat{A}_{x,m} \left|\psi\right\rangle_{AB} \left|2m\right\rangle_{A'} \left|2m\right\rangle_{B'} + X_{A,m} X_{B,m} P_B^{(2m+1)} \hat{A}_{x,m} \left|\psi\right\rangle_{AB} \left|2m+1\right\rangle_{A'} \left|2m+1\right\rangle_{B'} \Big) \\
=&X_B^{(2m)} X_A^{(2m)} \frac{1}{c_{2m}} P_B^{(2m)} \left|\psi\right\rangle_{AB} \otimes A_{x,m} \big(c_{2m} \left|2m\right\rangle_{A'} \left|2m\right\rangle_{B'} + c_{2m+1} \left|2m+1\right\rangle_{A'} \left|2m+1\right\rangle_{B'} \big) \\
=&\frac{1}{c_0} P_A^{(0)} \left|\psi\right\rangle_{AB} \otimes A_{x,m} \left|\psi_{\text{target}}\right\rangle = \left|\text{extra}\right\rangle \otimes A_{x,m} \left|\psi_{\text{target}}\right\rangle \ ,
\end{aligned}
$$

where the second-to-last line follows from the definitions of $X_{A,m}$ and $X_{B,m}$ in the main text, and from a proof following closely that in [7], that maximal violation of the tilted CHSH inequality self-tests the ideal single-qubit measurements. One obtains analogous statements involving $\hat{A}'_{0/1,m} = \Pi_{2m+1}^{A_{0/2}} - \Pi_{2m+2}^{A_{0/2}}$ and $\hat{B}'_{0/1,m} = \Pi_{2m+1}^{B_{2/3}} - \Pi_{2m+2}^{B_{2/3}}$.
From the above, we deduce that the measurements of Alice and Bob on $\left|\psi\right\rangle$ are equivalent under Φ, to the ideal measurements described in Subsection 5.1.2.3 on $\left|\psi_{\text{target}}\right\rangle$.

Appendix C

APPENDIX FOR "A GENERALIZATION OF THE CHSH INEQUALITY SELF-TESTING MAXIMALLY ENTANGLED STATES OF ANY LOCAL DIMENSION"

Robustness Obtaining a robust self-testing result is mainly a matter of going through the proof and replacing exact statements with approximate statements, where necessary. Here, we first state the robust self-testing theorem, then we give an outline of the proof pointing out the parts where it differs from the proof for the exact case.

Theorem 36 (Robust self-testing)**.** *Let $\mathcal{B}$ be the Bell operator from Definition* 32 *with parameters $d \geq 2, \delta > 0$. Let $\left(|\Psi\rangle, \{\tilde{\Pi}^a_{A_x}\}_a, \{\tilde{\Pi}^b_{B_y}\}_b\right)$ be the ideal strategy from Lemma 38, where $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$. There exists a constant $C > 0$ such that the following holds. Suppose the strategy $\left(|\psi\rangle, \{\Pi^a_{A_x}\}_a, \{\Pi^b_{B_y}\}_b\right)$ attains a correlation p such that $[\mathcal{B}]_p > 2\sqrt{2} - \epsilon$, for some $\epsilon < \frac{C}{d^3}$. Then, there exists a local unitary Φ and an auxiliary state $|aux\rangle$ such that*

$$\|\Phi(|\psi\rangle) - |\Psi\rangle \otimes |aux\rangle\| = O(d^6 \epsilon^{\frac{1}{8}})$$
$$\|\Phi(\Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle) - \tilde{\Pi}^a_{A_x} \otimes \tilde{\Pi}^b_{B_y} |\Psi\rangle \otimes |aux\rangle\| = O(d^6 \epsilon^{\frac{1}{8}}).$$

In the rest of this section we sketch the proof of Theorem 36. In doing so, we will state approximate versions of Lemma 39 and 40 from the main text.

Lemma 54 (Approximate version of Lemma 39)**.** *Let $\mathcal{B}$ be the Bell operator with parameters $d \geq 2$ and $\delta > 0$. Let $p \in \mathcal{C}_q^{3,4,d,d}$ be a quantum correlation such that $[\mathcal{B}]_p > 2\sqrt{2} - \epsilon$. Then, $p(a,b|x,y) < \frac{2}{\delta}\epsilon$ for all $(a,b,x,y) \in \mathcal{C} \cup \mathcal{C}'$, where $\mathcal{C}$ and $\mathcal{C}'$ are as in equations* (5.17) *and* (5.18).

Proof. The proof is very similar to the proof of Lemma 39. The only difference is that we now suppose for a contradiction that p is such that $[\mathcal{B}]_p > 2\sqrt{2} - \epsilon$ and $p(a,b|x,y) \geq \frac{2}{\delta}\epsilon$ for some $(a,b,x,y) \in \mathcal{C} \cup \mathcal{C}'$. Then in order to compensate for a negative contribution $\geq \delta \cdot \frac{2}{\delta}\epsilon = 2\epsilon$, it must be that either $\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}_m]_p > 2\sqrt{2}$ or $\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}'_m]_p > 2\sqrt{2}$. In either case, analogously to the proof of Lemma 39, one can reduce this to a strategy that wins CHSH with value $> 2\sqrt{2}$. □

Lemma 55 (Approximate version of Lemma 40)**.** *Any correlation $p \in \mathcal{C}_q^{3,4,d,d}$ such that each cross term has size $O(\epsilon)$ (i.e. of the form of Lemma 54 - we are thinking of δ as a constant), induced by some strategy $\left(|\psi\rangle, \{\Pi^a_{A_x}\}_a, \{\Pi^b_{B_y}\}_b\right)$, satisfies the following:*

- *If d is even, then for each $m = 0, .., \frac{d}{2} - 1$, there exist weights $w_m, w'_m \geq 0$ with $1 - O(\epsilon) \leq \sum_m w_m, \sum_m w'_m \leq 1$, and correlations $p_m, p'_m \in \mathcal{C}_q^{2,2,2,2}$ (with questions in $\{0,1\}^2$ and $\{0,2\} \times \{2,3\}$ respectively, and answers in $\{0,1\}$) such that $\forall m$, $\forall a, b \in \{2m, 2m+1\}, x, y \in \{0,1\}$:*

$$p(a,b|x,y) \approx_{O(\epsilon)} w_m \cdot p_m(a \mod 2, b \mod 2|x,y) \approx_{O(\epsilon)} \langle\psi| \Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle$$

and $\forall m$, $\forall a, b \in \{2m+1, 2m+2\}, x \in \{0,2\}, y \in \{2,3\}$:

$$p(a,b|x,y) \approx_{O(\epsilon)} w'_m \cdot p'_m(a \mod 2, b \mod 2|x,y) \approx_{O(\epsilon)} \langle\psi| \Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle$$

.

- *If d is odd, the analogous statement holds, except that the weights w_m, w'_m are such that $1 - O(\epsilon) \leq \sum_m w_m + p(d-1, d-1|0,0), \sum_m w'_m + p(0,0|2,2) \leq 1 + O(\epsilon)$, AND*
  - $p(d-1, d-1|x,y) \approx_{O(\epsilon)} p(d-1, d-1|x',y') \ \forall x, y, x'y' \in \{0,1\}$
  - $p(0,0|x,y) \approx_{O(\epsilon)} p(0,0|x',y') \ \forall x, x' \in \{0,2\}, y, y' \in \{2,3\}$

Proof. All equalities from (5.22) to (5.23) now hold approximately, up to addition of orthogonal vectors of norm $O(\sqrt{\epsilon})$. The weights w_m are defined in the same way as in the proof of Lemma 40. The main difference is that now correlation p_m is defined to be any correlation such that $w_m \cdot p_m(a \mod 2, b \mod 2|x,y) \approx_{O(\epsilon)} \langle\psi| \Pi^a_{A_x} \otimes \Pi^b_{B_y} |\psi\rangle$ for all $a, b \in \{2m, 2m+1\}, x, y \in \{0,1\}$ (note that with an exact equality p_m would not be a well-defined correlation, but an $O(\epsilon)$ correction is enough for existence of such a correlation p_m). We argue similarly for w'_m and p'_m. The case of d odd is also similar. □

Proof of Theorem 36. We look at the case of d even first. Using Lemma 55, we deduce

$$\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}_m]_p \approx_{O(d\epsilon)} \sum_{m=0}^{\frac{d}{2}-1} w_m \cdot [\mathrm{CHSH}]_{p_m} \leq 2\sqrt{2}$$
$$\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}'_m]_p \approx_{O(d\epsilon)} \sum_{m=0}^{\frac{d}{2}-1} w'_m \cdot [\mathrm{CHSH}]_{p_m} \leq 2\sqrt{2}\,.$$

Hence,

$$\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}_m]_p \leq 2\sqrt{2} + O(d\epsilon) \tag{C.1}$$
$$\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}'_m]_p \leq 2\sqrt{2} + O(d\epsilon)\,. \tag{C.2}$$

It is straightforward to see that (C.1) and (C.2) imply the existence of constants $C', C'' > 0$ such that

- for all m, $w_m \leq C'\sqrt{d\epsilon}$ OR $[\text{CHSH}]_{p_m} \geq 2\sqrt{2} - C''\sqrt{d\epsilon}$, AND
- for all m, $w'_m \leq C'\sqrt{\epsilon}$ OR $[\text{CHSH}]_{p'_m} \geq 2\sqrt{2} - C''\sqrt{\epsilon}$.

From here, we deduce approximate equations like $\|\Pi_{A_0}^{2m+1}|\psi\rangle\|^2 \approx_{O(\sqrt{d\epsilon})} w_m \cdot \frac{1}{2}$ and $\|\Pi_{A_0}^{2m+1}|\psi\rangle\|^2 \approx_{O(\sqrt{d\epsilon})} w'_m \cdot \frac{1}{2}$, and similar other equations as in the proof of Theorem 18. These follow from a robust self-testing bound on CHSH. Now, such approximate equations imply, by applying triangle inequalities, that, for all m,

$$w_m \approx_{O(d^{3/2}\sqrt{\epsilon})} w'_m \approx_{O(d^{3/2}\sqrt{\epsilon})} \frac{2}{d}. \tag{C.3}$$

It is clear that there exists a constant $C > 0$ such that for $\epsilon < \frac{C}{d^3}$, it must be that for all m $w_m > C'\sqrt{d\epsilon}$ and $w'_m > C'\sqrt{d\epsilon}$. Hence, for $\epsilon < \frac{C}{d^3}$, it is the case that, for all m,

$$[\text{CHSH}]_{p_m}, [\text{CHSH}]_{p'_m} \geq 2\sqrt{2} - C''\sqrt{d\epsilon}. \tag{C.4}$$

Finally, recall the form of correlation p from Lemma 55. This, combined with (C.3) and (C.4) implies that p is $O(d^2\sqrt{\epsilon})$-close to the ideal correlation $\tilde{p}$ defined by the measurements of Lemma 38 (i.e. for all a, b, x, y, $p(a,b|x,y) \approx_{O(d^2\sqrt{\epsilon})} \tilde{p}(a,b,|x,y)$, where $\tilde{p}$ is the ideal correlation). The robust self-testing statement from [25] for the ideal correlation of Lemma 38 states that a strategy producing a correlation that is ϵ-close to ideal, must be $O(d^3\epsilon^{\frac{1}{4}})$-close (in the sense of Theorem 36) to the ideal strategy. Applying this to our analysis yields the conclusion of Theorem 36.

The case of d odd is handled similarly.

□

Appendix D

APPENDIX FOR "SELF-TESTING MULTIPARTITE STATES THROUGH PROJECTION ONTO TWO SYSTEMS"

D.1 Proof of Theorem 19

For ease of exposition, we prove the Theorem in the case $N = 4$, with the extension to general N being immediate.

Let $A_0, A_1, B_0, B_1, C_0, C_1, D_0, D_1$, be the pairs of observables for the four parties. For an observable D, let $P_D^a = [\mathbb{1} + (-1)^a D]/2$, and for brevity let c_θ and s_θ denote respectively $\cos\theta$ and $\sin\theta$. For clarity, we recall the correlations from Theorem 19, for the case $N = 4$:

$$\begin{aligned}
&\langle\psi| \quad P^0_{A_0}|\psi\rangle = \langle\psi| P^0_{B_0}|\psi\rangle = \langle\psi| P^0_{C_0}|\psi\rangle = \langle\psi| P^0_{A_0}P^0_{C_0}|\psi\rangle = \langle\psi| P^0_{B_0}P^0_{C_0}|\psi\rangle = c_\theta^2, \\
&\langle\psi| \quad P^a_{A_1}P^b_{B_1}|\psi\rangle = \frac{1}{4}, \ \text{for } a,b \in 0,1 \\
\langle\psi| P^a_{A_1} \quad P^b_{B_1} \quad &\left(\beta C_0 + C_0D_0 + C_0D_1 + (-1)^{a+b}(C_1D_0 - C_1D_1)\right)|\psi\rangle = \frac{\sqrt{8+2\beta^2}}{4}, \ \text{for } a,b \in 0,1\,,
\end{aligned}$$

where $\tan 2\theta = \sqrt{\frac{2}{\beta^2} - \frac{1}{2}}$. Equations (D.1a) imply, by Cauchy-Schwartz inequality, that

$$P^0_{A_0}|\psi\rangle = P^0_{B_0}|\psi\rangle = P^0_{C_0}|\psi\rangle$$

and consequently

$$P^1_{A_0}|\psi\rangle = P^1_{B_0}|\psi\rangle = P^1_{C_0}|\psi\rangle\,.$$

Notice that equation (D.1b) implies $\|P^a_{A_1}P^b_{B_1}|\psi\rangle\| = 1/2$, for $a,b \in \{0,1\}$, and that the equations in (D.1c) describe maximal violations of tilted CHSH inequalities by the normalized state $2P^a_{A_1}P^b_{B_1}|\psi\rangle$, for $a,b \in \{0,1\}$ (the ones for $a \oplus b = 1$ are tilted CHSH inequalities upon relabelling $D_1 \to -D_1$).

Let μ be such that $\tan\mu = s_{2\theta}$. Define $X_A := A_1, X_B := B_1$ and $X_C := C_1$. Then, let $Z'_D = (D_0 + D_1)/2\cos\mu$, and let Z^*_D be Z'_D where we have replaced the zero eigenvalues with 1. Define $Z_D = Z^*_D|Z^*_D|^{-1}$. Define X_D similarly starting from $X'_D = (D_0 - D_1)/2\cos\mu$. Let $P^a_{Z_D} = [\mathbb{1} + (-1)^a Z_D]/2$. The maximal violations of tilted CHSH from (D.1c) imply, thanks to Lemma 1 41, that

$$\begin{aligned}
P^a_{C_0} &= P^a_{Z_D}, \qquad \text{for } a \in \{0,1\}, \\
s_\theta P^a_{A_1}P^b_{B_1}X_CX_DP^0_{C_0}|\psi\rangle &= (-1)^{a+b}c_\theta P^a_{A_1}P^b_{B_1}P^1_{C_0}|\psi\rangle\,, \ \text{for } a,b \in \{0,1\}. \qquad \text{(D.2)}
\end{aligned}$$

If we introduce notation $X_A = A_1, X_B = B_1$ and $X_C = C_1$, then

$$\begin{aligned} X_A X_B X_C X_D P^1_{A_0} |\psi\rangle &= (P^0_{A_1} - P^1_{A_1})(P^0_{B_1} - P^1_{B_1}) X_C X_D P^1_{C_0} |\psi\rangle \\ &= P^0_{A_1} P^0_{B_1} X_C X_D P^1_{C_0} |\psi\rangle - P^0_{A_1} P^1_{B_1} X_C X_D P^1_{C_0} |\psi\rangle - P^1_{A_1} P^0_{B_1} X_C X_D P^1_{C_0} |\psi\rangle \\ &\quad + P^1_{A_1} P^1_{B_1} X_C X_D P^1_{C_0} |\psi\rangle \\ &= \frac{s_\theta}{c_\theta} P^0_{A_1} P^0_{B_1} P^0_{A_0} |\psi\rangle + \frac{s_\theta}{c_\theta} P^0_{A_1} P^1_{B_1} P^0_{A_0} |\psi\rangle + \frac{s_\theta}{c_\theta} P^0_{A_1} P^1_{B_1} P^0_{A_0} |\psi\rangle + \frac{s_\theta}{c_\theta} P^1_{A_1} P^1_{B_1} P^0_{A_0} |\psi\rangle \\ &= \frac{s_\theta}{c_\theta} P^0_{A_0} |\psi\rangle , \end{aligned}$$

where we used equation (D.2) to obtain the third line, and $\sum_{a,b\in\{0,1\}} P^a_{A_1} P^b_{B_1} = \mathbb{1}$ to obtain the last. Conditions (5.25) and (5.26) of Theorem 19 follow immediately from the above.

D.2 Proof of Lemma 42

In this section, we provide a proof of Lemma 42. We explicitly construct a local isometry Φ such that $\Phi(|\psi\rangle) = |extra\rangle \otimes |\Psi\rangle$ for any Schmidt state $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle^{\otimes N}$, where $0 < c_j < 1$ for all j and $\sum_{j=0}^{d-1} c_j^2 = 1$, and $|extra\rangle$ is some auxiliary state.

Proof. Recall that $\{P^{(k)}_l\}_{k=0}^{d-1}$ are complete sets of orthogonal projections for $l = 1, \ldots, N-1$ by hypothesis. Then, notice that for $i \neq j$ we have, using condition (5.1), $P^{(i)}_N P^{(j)}_N |\psi\rangle = P^{(i)}_N P^{(j)}_1 |\psi\rangle = P^{(j)}_1 P^{(i)}_1 |\psi\rangle = 0$, i.e., the $P^{(k)}_N$ are "orthogonal when acting on $|\psi\rangle$".

Let $\mathcal{A}$ be the unital algebra generated by $\{P^{(k)}_1\}$. Let $\mathcal{H}' = \mathcal{A}|\psi\rangle$, where $\mathcal{A}|\psi\rangle = \{Q|\psi\rangle : Q \in \mathcal{A}\}$. Let $\tilde{P}^{(k)}_N = P^{(k)}_N|_{\mathcal{H}'}$ be the restriction of $P^{(k)}_N$ to $\mathcal{H}'$. Then, $\{\tilde{P}^{(k)}_N\}_{k=0}^{d-1}$ is a set of orthogonal projections. This is because, thanks to (5.1), one can always move the relevant operators to be in front of $|\psi\rangle$, as in the simple example

$$\tilde{P}^{(i)}_N \tilde{P}^{(j)}_N (P^{(k)}_1 |\psi\rangle') = P^{(k)}_1 \tilde{P}^{(i)}_N \tilde{P}^{(j)}_N |\psi\rangle = 0.$$

Thus, the set $\{\tilde{P}^{(k)}_B, I - P'_B\}$, where P'_B is the sum of all other projections, is a complete set of orthogonal projections.

Now, define $Z_l := \sum_{k=0}^{d-1} \omega^k P^{(k)}_l$, for $l = 1, \ldots, N-1$, and $Z_N := \sum_{k=0}^{d-1} \omega^k \tilde{P}^{(k)}_N + \mathbb{1} - \sum_{k=0}^{d-1} \tilde{P}^{(k)}_N$. In particular, the Z_l are all unitary. Notice, moreover, that $\left(\mathbb{1} - \sum_k \tilde{P}^{(k)}_N\right)|\psi\rangle = 0$, by using (5.1) and the fact that the $\{P^{(k)}_l\}$ are complete.

Define the local isometry

$$\Phi := \bigotimes_{l=1}^{N} R_{ll'} \bar{F}_{l'} S_{ll'} F_{l'} \mathrm{App}_l,$$

where $\mathrm{App}_l : \mathcal{H}_l \to \mathcal{H}_l \otimes \mathcal{H}_{l'}$ is the isometry that simply appends $|0\rangle_{l'}$, F is the quantum Fourier transform, $\bar{F}$ is the inverse quantum Fourier transform, $R_{ll'}$ is defined so that $|\phi\rangle_l |k\rangle_{l'} \mapsto X_l^{(k)} |\phi\rangle_l |k\rangle_{l'} \ \ \forall |\phi\rangle$, and $S_{ll'}$ is defined so that $|\phi\rangle_l |k\rangle_{l'} \mapsto Z_l^k |\phi\rangle_l |k\rangle_{l'} \ \ \forall |\phi\rangle$. We compute the action of Φ on $|\psi\rangle$. For ease of notation with drop the tildes from the $\tilde{P}_N^{(k)}$, while still referring to the new orthogonal projections.

$$
\begin{aligned}
|\psi\rangle \otimes |0\rangle^{\otimes N} &\xrightarrow{\otimes_l F_{l'}} \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} |\psi\rangle \otimes \bigotimes_l |k_l\rangle_{l'} \\
&\xrightarrow{\otimes_l S_{ll'}} \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} \left[\prod_{i=1}^{N-1} \left(\sum_{j_i} \omega^{j_i} P_i^{(j_i)} \right)^{k_i} \right] \left(\sum_{j_N} \omega^{j_N} P_N^{(j_N)} + \mathbb{1} - \sum_k P_N^{(j_N)} \right)^{k_N} |\psi\rangle \otimes \bigotimes_l |k_l\rangle_{l'} \\
&= \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} \sum_{j_1,\ldots,j_N} \prod_{i=1}^{N} \omega^{j_i k_i} P_i^{(j_i)} |\psi\rangle \otimes \bigotimes_l |k_l\rangle_{l'} \\
&= \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} \sum_{j_1,\ldots,j_N} \prod_{i=1}^{N} \omega^{j_i k_i} P_1^{(j_i)} |\psi\rangle \otimes \bigotimes_l |k_l\rangle_{l'} \\
&= \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} \sum_j \omega^{j(\sum_i k_i)} P_1^{(j)} |\psi\rangle \otimes \bigotimes_l |k_l\rangle_{l'} \\
&\xrightarrow{\otimes_l \bar{F}_{l'}} \frac{1}{d^N} \sum_{k_1,\ldots,k_N} \sum_j \sum_{m_1,\ldots,m_N} \omega^{j(\sum_i k_i)} \prod_r \omega^{-m_r k_r} P_1^{(j)} |\psi\rangle \otimes \bigotimes_l |m_l\rangle_{l'} \\
&= \frac{1}{d^N} \sum_{k_1,\ldots,k_N} \sum_j \sum_{m_1,\ldots,m_N} \prod_i \omega^{k_i (j - m_i)} P_1^{(j)} |\psi\rangle \otimes \bigotimes_l |m_l\rangle_{l'} \\
&= \sum_j P_1^{(j)} |\psi\rangle \otimes |j\rangle^{\otimes N} \\
&\xrightarrow{\otimes_l R_{ll'}} \sum_j \left(\prod_i X_i^{(j)} \right) P_1^{(j)} |\psi\rangle \otimes |j\rangle^{\otimes N} \\
&= \sum_j \frac{c_j}{c_0} P_1^{(0)} |\psi\rangle \otimes |j\rangle^{\otimes N} \qquad \text{(D.5)} \\
&= \frac{1}{c_0} P_1^{(0)} |\psi\rangle \otimes \sum_j c_j |j\rangle^{\otimes N} \\
&= |\text{extra}\rangle \otimes |\psi_{\text{target}}\rangle \,,
\end{aligned}
$$

where to get (D.5) we used condition (5.1). It is an easy check to see that the whole proof above can be repeated by starting from a mixed joint state, yielding a corresponding version of the Lemma that holds for a general mixed state. □

D.3 Proof of Theorem 20

As mentioned, we work in the tripartite case, as the general n-partite case follows analogously. The measurements of Alice, Bob and Charlie can be assumed to be projective, since we make no assumption on the dimension of the system. For ease of notation, the proof assumes that the joint state is pure, but one easily realizes that the proof goes through in the same way by rephrasing everything in terms of density matrices (see [23] for a slightly more detailed discussion).

Let $|\psi\rangle$ be the unknown joint state, and let $P^a_{A_x}$ be the projection on Alice side corresponding obtaining outcome a on question x. Define $P^b_{B_y}$ and $P^c_{C_z}$ similarly on Bob and Charlie's side. The proof structure follows closely that of [23], and goes through explicitly constructing projectors and unitary operators satisfying the sufficient conditions of Lemma 42.

Define $\hat{A}_{x,m} = P^{2m}_{A_x} - P^{2m+1}_{A_x}$, $\hat{B}_{y,m} = P^{2m}_{B_y} - P^{2m+1}_{B_y}$ and $\hat{C}_{z,m} = P^{2m}_{C_z} - P^{2m+1}_{C_z}$, for $x, y, z \in \{0,1\}$. Let $\mathbb{1}^m_{A_x} = P^{2m}_{A_x} + P^{2m+1}_{A_x}$ and similarly define $\mathbb{1}^m_{B_y}$ and $\mathbb{1}^m_{C_z}$ for $x, y, z \in \{0,1\}$. Now,

$$\begin{aligned} \|P^{2m}_{A_0}\| &= \sqrt{\left\langle \psi \middle| P^{2m}_{A_0} \right\rangle \psi} \\ &= \sqrt{\left\langle \psi \middle| P^{2m}_{A_0} \textstyle\sum_{i=0}^{d-1} P^i_{B_0} \sum_{j=0}^{d-1} P^j_{C_0} \right\rangle \psi} \\ &= c_{2m}, \end{aligned}$$

and $\|P^{2m+1}_{A_0}\| = c_{2m+1}$. Similarly, we derive $\|\mathbb{1}^m_{A_x}|\psi\rangle\| = \|\mathbb{1}^m_{B_y}|\psi\rangle\| = \|\mathbb{1}^m_{C_z}|\psi\rangle\| = (c^2_{2m} + c^2_{2m+1})^{1/2}$ for any m and $x, y, z \in \{0,1\}$. Notice then that

$$\begin{aligned} \left\langle \psi \middle| \mathbb{1}^m_{A_x}\mathbb{1}^m_{B_y} \right\rangle \psi &= \left\langle \psi \middle| \mathbb{1}^m_{A_x}\mathbb{1}^m_{B_y} \textstyle\sum_{i=0}^{d-1} P^i_{C_0} \right\rangle \psi \\ &= \left\langle \psi \middle| \mathbb{1}^m_{A_x}\mathbb{1}^m_{B_y}\mathbb{1}^m_{C_0} \right\rangle \psi \\ &= c^2_{2m} + c^2_{2m+1}, \end{aligned}$$

where the second last equality is from the block-diagonal structure of the correlations. Since $\|\mathbb{1}^m_{A_x}|\psi\rangle\| = \|\mathbb{1}^m_{B_y}|\psi\rangle\| = (c^2_{2m} + c^2_{2m+1})^{1/2}$, then Cauchy-Schwartz inequality implies $\mathbb{1}^m_{A_x}|\psi\rangle = \mathbb{1}^m_{B_y}|\psi\rangle$. So, we have

$$\mathbb{1}^m_{A_x}|\psi\rangle = \mathbb{1}^m_{B_y}|\psi\rangle = \mathbb{1}^m_{C_z}|\psi\rangle \tag{D.8}$$

for all $x, y, z \in \{0,1\}$. The correlations are, by design, such that $\hat{A}_{0,m}, \hat{A}_{1,m}, \hat{B}_{0,m}, \hat{B}_{1,m}, \hat{C}_{0,m}, \hat{C}_{0,m}$, the associated projections $P^j_{A_i}, P^j_{B_i}, P^j_{C_i}$, $j \in \{2m, 2m+1\}$ and $|\psi\rangle$ reproduce the correlations $(c^2_{2m} + c^2_{2m+1}) \cdot C^{\mathrm{ghz}_{3,2,\theta_m}}_{x,y,z}$. In order to apply Theorem 19, we need to define the normalized state $|\psi'_m\rangle := (\mathbb{1}^m_{A_0}|\psi\rangle)/(c^2_{2m} + c^2_{2m+1})^{1/2}$ and the "unitarized" versions of the operators above,

namely $\hat{D}_{i,m} := \mathbb{1} - \mathbb{1}_m^{D_i} + \hat{D}_{i,m}$, for $D \in \{A, B, C\}$. It is easy to check that then $\hat{A}_{i,m}$, $\hat{B}_{i,m}$ and $\hat{C}_{i,m}$ satisfy the conditions of Theorem 19 (for $N = 3$) on state $|\psi'_m\rangle$. Thus, letting we have that,

$$Z_{A,m} |\psi'_m\rangle = Z_{B,m} |\psi'_m\rangle = Z_{C,m} |\psi'_m\rangle , \tag{D.9}$$

$$X_{A,m}X_{B,m}X_{C,m}(\mathbb{1} - Z_{A,m}) |\psi'_m\rangle = \tan(\theta_m)(\mathbb{1} + Z_{A,m}) |\psi'_m\rangle . \tag{D.10}$$

Define the subspace $\mathcal{C}_m = \text{range}(\mathbb{1}_m^{C_0}) + \text{range}(\mathbb{1}_m^{C_1})$, and the projection $\mathbb{1}_{\mathcal{C}_m}$ onto subspace $\mathcal{C}_m$. Then, notice from the way $Z_{C,m}$ is defined, that it can be written as $Z_{C,m} = \mathbb{1} - \mathbb{1}_{\mathcal{C}_m} + \tilde{Z}_{C,m}$, where $\tilde{Z}_{C,m}$ is some operator living entirely on subspace $\mathcal{C}_m$. This implies that $Z_{C,m} |\psi_m\rangle = \tilde{Z}_{C,m} |\psi_m\rangle = \tilde{Z}_{C,m} |\psi\rangle$, where we have used (D.8) and the fact that

$$\mathbb{1}_m^{C_0} |\psi\rangle = \mathbb{1}_m^{C_1} |\psi\rangle \implies \mathbb{1}_{\mathcal{C}_m} |\psi\rangle = \mathbb{1}_m^{C_i} |\psi\rangle .$$

Hence, from (D.9) it is not difficult to deduce that $\hat{A}_{0,m} |\psi\rangle = \hat{B}_{0,m} |\psi\rangle = \tilde{Z}_{C,m} |\psi\rangle$.

Constructing the projections of Lemma 42. Define projections $P_A^{(2m)} := (\mathbb{1}_m^{A_0} + \hat{A}_{0,m})/2 = P_{A_0}^{2m}$, $P_A^{(2m+1)} := (\mathbb{1}_m^{A_0} - \hat{A}_{0,m})/2 = P_{A_0}^{2m+1}$, $P_B^{(2m)} := (\mathbb{1}_m^{B_0} + \hat{B}_{0,m})/2 = P_{B_0}^{2m}$, $P_B^{(2m+1)} := (\mathbb{1}_m^{B_0} - \hat{B}_{0,m})/2 = P_{B_0}^{2m+1}$, $P_C^{(2m)} := (\mathbb{1}_{\mathcal{C}_m} + \tilde{Z}_{C,m})/2$ and $P_C^{(2m+1)} := (\mathbb{1}_{\mathcal{C}_m} - \tilde{Z}_{C,m})/2$.

Note that $P_C^{(2m)}$, $P_C^{(2m+1)}$ are indeed projections, since $\tilde{Z}_{C,m}$ has all ± 1 eigenvalues corresponding to subspace $\mathcal{C}_m$, and is zero outside. We also have, for all m and $k = 2m, 2m+1$,

$$\begin{aligned} P_B^{(k)} |\psi\rangle = P_A^{(k)} |\psi\rangle = \frac{1}{2}[\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m}] |\psi\rangle = \frac{1}{2}[\mathbb{1}_m^{B_0} + (-1)^k \hat{A}_{0,m}] |\psi\rangle \\ = \frac{1}{2}[\mathbb{1}_{\mathcal{B}_m} + (-1)^k \tilde{Z}_{B,m}] |\psi\rangle = P_C^{(k)} |\psi\rangle . \end{aligned}$$

Further, notice that $[\mathbb{1} + (-1)^k Z_{A,m}] |\psi'_m\rangle = [\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m}] |\psi'_m\rangle = [\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m}] |\psi\rangle = P_A^{(k)} |\psi\rangle$. Substituting this into (D.10), gives

$$X_{A,m}X_{B,m}X_{C,m}P_A^{(2m+1)} |\psi\rangle = \tan(\theta_m)P_A^{(2m)} |\psi\rangle = \frac{c_{2m+1}}{c_{2m}} P_A^{(2m)} |\psi\rangle . \tag{D.12}$$

Now, for the "shifted" blocks, we can similarly define $\hat{A}'_{x,m}$, $\hat{B}'_{x,m}$ and $\hat{C}'_{x,m}$ as $\hat{A}_{x,m} = P_{A_x}^{2m+1} - P_{A_x}^{2m+2}$ and similar. Then, analogously, we deduce the existence of hermitian and unitary operators $Y'_{A,m}$, $Y'_{B,m}$ and $Y'_{C,m}$ such that

$$Y_{A,m}Y_{B,m}Y_{C,m}P_A^{(2m+2)} |\psi\rangle = \frac{c_{2m+2}}{c_{2m+1}} P_A^{(2m+1)} |\psi\rangle . \tag{D.13}$$

Constructing the unitary operators of Lemma 42. We will now directly construct unitary operators satisfying conditions (5.1,42) of Lemma 42. Define $X^{(k)}_{A/B/C}$ as follows:

$$X^{(k)}_A = \begin{cases} \mathbb{1}, & \text{if } k = 0, \\ X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}Y_{A,m-1}X_{A,m}, & \text{if } k = 2m+1, \\ X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\dots X_{A,m-1}Y_{A,m-1}, & \text{if } k = 2m, \end{cases}$$

and analogously for $X^{(k)}_B$ and $X^{(k)}_C$. Note that $X^{(k)}_A$ and $X^{(k)}_B$ are unitary since they are product of unitaries. Finally, we are left to check that

$$X^{(k)}_A X^{(k)}_B X^{(k)}_C P^{(k)}_A \left|\psi\right\rangle = \frac{c_k}{c_0} P^{(0)}_A \left|\psi\right\rangle . \tag{D.14}$$

The case $k = 0$ holds trivially. For $k = 2m+1$, For $k = 2m+1$,

$$\begin{aligned} &X^{(k)}_A X^{(k)}_B X^{(k)}_C P^{(k)}_A \left|\psi\right\rangle \\ &\quad = X_{A,0}Y_{A,0}X_{B,0}Y_{B,0}X_{C,0}Y_{C,0}\dots X_{A,m-1}Y_{A,m-1}X_{B,m-1}Y_{B,m-1}X_{C,m-1}Y_{C,m-1} \\ &\qquad \times X_{A,m}X_{B,m}X_{C,m}P^{(2m+1)}_A \left|\psi\right\rangle \\ &\quad \overset{(D.12)}{=} \frac{c_{2m+1}}{c_{2m}} X_{A,0}Y_{A,0}X_{B,0}Y_{B,0}X_{C,0}Y_{C,0}\dots X_{A,m-1}Y_{A,m-1}X_{B,m-1}Y_{B,m-1}X_{C,m-1}Y_{C,m-1}P^{(2m)}_A \left|\psi\right\rangle \\ &\quad \overset{(D.13)}{=} \frac{c_{2m+1}}{c_{2m}} \cdot \frac{c_{2m}}{c_{2m-1}} X_{A,0}Y_{A,0}X_{B,0}Y_{B,0}X_{C,0}Y_{C,0}\dots X_{A,m-2}Y_{A,m-2}X_{B,m-2}Y_{B,m-2} \\ &\qquad \times X_{C,m-2}Y_{C,m-2}P^{(2m-1)}_A \left|\psi\right\rangle \\ &\quad = \dots \\ &\quad = \frac{c_{2m+1}}{\cancel{c_{2m}}} \cdot \frac{\cancel{c_{2m}}}{\cancel{c_{2m-1}}} \dots \frac{\cancel{c_2}}{\cancel{c_1}} \cdot \frac{\cancel{c_1}}{c_0} P^{(0)}_A \left|\psi\right\rangle \\ &\quad = \frac{c_{2m+1}}{c_0} P^{(0)}_A \left|\psi\right\rangle , \end{aligned}$$

which is indeed (D.14) as $2m+1 = k$. The case $k = 2m$ is similar. This concludes the proof of Theorem 20.